特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004年7月29日 (29.07.2004)

PCT

(10) 国際公開番号
WO 2004/064314 A1

(51) 国際特許分類[7]: H04L 9/10, G11B 20/10, 20/12

(21) 国際出願番号: PCT/JP2003/016937

(22) 国際出願日: 2003年12月26日 (26.12.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-006916 2003年1月15日 (15.01.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 木谷 聡 (KITANI,Satoshi) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 村松 克美 (MURAMATSU,Katsumi) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

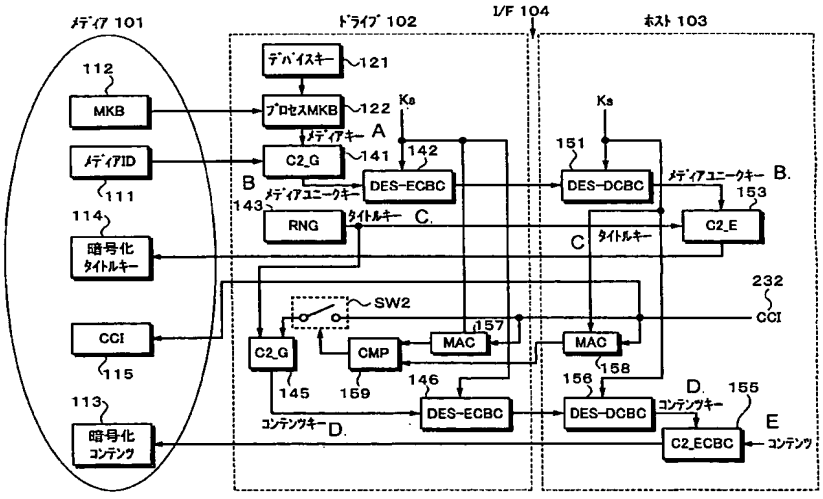
(74) 代理人: 杉浦 正知, 外(SUGIURA,Masatomo et al.); 〒171-0022 東京都 豊島区 南池袋2丁目49番7号 池袋パークビル７階 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,

[続葉有]

(54) Title: SIGNAL PROCESSING SYSTEM, RECORDING METHOD, PROGRAM, RECORDING MEDIUM, REPRODUCTION DEVICE, AND INFORMATION PROCESSING DEVICE

(54) 発明の名称: 信号処理システム



101...MEDIUM
111...MEDIUM ID
114...ENCRYPTION TITLE KEY
113...ENCRYPTED CONTENT
102...DRIVE
121...DEVICE KEY
122...PROCESS MKB
A...MEDIUM KEY
B...MEDIUM UNIQUE KEY
C...TITLE KEY
D...CONTENT KEY
103...HOST
E...CONTENT

(57) Abstract: A recorder consists of a drive (102) and a host (103) performing mutual authentication. C2_G (141) of the drive (102) is transferred to the host (103) after a medium unique key calculated by the medium ID and a medium key is encrypted by using a session key (Ks) generated by mutual authentication. A title key generated by a random number generator (143) of the drive (102) is transferred to the host (103). C2_G (145) of the drive (102) is transferred to the host (103) after the content key calculated from the title key and the CCI (232) is encrypted by using the session key (Ks). By using the content key decrypted by the host (103), the content is encrypted and the drive (102) records the encrypted content, encryption title key, and the CCI (232) onto a medium (101).

(57) 要約: 相互認証を行うドライブ１０２とホスト１０３とからレコーダが構成される。ドライブ１０２のＣ２Ｇ１４１がメディアＩＤとメディアキーから計算したメディアユニークキーが相互認証によって生成したセッションキーＫｓを用いて暗号化されてからホスト１０３に転送される。

[続葉有]

WO 2004/064314 A1

LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

ドライブ１０２の乱数発生器１４３が発生したタイトルキーがホスト１０３に転送される。ドライブ１０２のＣ２Ｇ１４５がタイトルキーとＣＣＩ２３２とから計算したコンテンツキーがセッションキーＫｓを用いて暗号化されてからホスト１０３へ転送される。ホスト１０３が復号したコンテンツキーを用いてコンテンツを暗号化し、ドライブ１０２が暗号化コンテンツ、暗号化タイトルキーおよびＣＣＩ２３２をメディア１０１へ記録する。

明 細 書

信号処理システム

技術分野

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号化コンテンツを再生する場合に適用される信号処理システム、記録方法、プログラム、記録媒体、再生装置および情報処理装置に関する。

背景技術

近年開発されたＤＶＤ(Digital Versatile Disc)等の記録媒体では、１枚の媒体に例えば映画１本分の大量のデータをディジタル情報として記録することが可能である。このように映像情報等をディジタル情報として記録することが可能となってくると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

ＤＶＤ－Video では、コピープロテクション技術としてＣＳＳ(Content Scrambling System) が採用されている。ＣＳＳは、ＤＶＤ－ＲＯＭメディアに対する適用のみが認可されており、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷ、ＤＶＤ＋Ｒ、ＤＶＤ＋ＲＷ等の記録型ＤＶＤでのＣＳＳの利用がＣＳＳ契約によって禁止されている。したがって、ＣＳＳ方式で著作権保護されたＤＶＤ－Video の内容を記録型ＤＶＤへのまるごとコピー（ビットバイビットコピー）することは、ＣＳＳ契約上では、認められた行為ではない。

しかしながら、ＣＳＳの暗号方式が破られる事態が発生した。ＣＳＳの暗号化を解除してＤＶＤ－Video の内容を簡単にハードディスクにコピーすることを可能とする「ＤｅＣＳＳ」と呼ばれるソフトウェアがインターネット上で配布された。「ＤｅＣＳＳ」が出現した背景には、本来耐タンパー化が義務付けられているはずのＣＳＳ復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にＣＳＳアルゴリズム全体が解読された経緯がある。

ＣＳＳの後に、ＤＶＤ－Audio 等のＤＶＤ－ＲＯＭの著作権保護技術であるＣＰＰＭ(Content Protection for Pre-Recorded Media)、並びに記録型ＤＶＤ、メモリカードに関する著作権保護技術ＣＰＲＭ(Content Protection for Recordable Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、データをまるごとコピーしても再生を制限できる特徴を有している。ＤＶＤに関する著作権保護の方法に関しては、下記の非特許文献１に説明され、ＣＰＲＭは、ライセンス管理者である米4C Entity, LLC が配布する下記の資料に説明されている。

山田，「ＤＶＤを起点に著作権保護空間を広げる」，日経エレクトロニクス 2001.8.13, p.143-153

"Content Protection for Recordable Media Specification DVD Book"、インターネット＜ＵＲＬ：http://www.4Centity.com/＞

パーソナルコンピュータ（以下、適宜ＰＣと略す）環境下では、ＰＣとドライブとが標準的インターフェースで接続されるために、標準的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。アプリケーションソフトウェア

がリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

著作権保護技術をＰＣ上で実行されるアプリケーションプログラムへ実装する際には、その著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的である。しかしながら、耐タンパー性の強度を示す指標がない。その結果、どの程度のリバースエンジニアリングへの対応を行うかは、インプレメンターの個々の判断や能力に委ねられているのが現状である。ＣＳＳの場合は、結果としてその著作権保護技術が破られてしまった。ＣＳＳの後に提案されたＣＰＰＭおよび記録型ＤＶＤに関する著作権保護技術ＣＰＲＭにおいても、既に破られているＣＳＳに新たな機能を加えたものであり、また、著作権保護技術に関わるアルゴリズムは、大部分がＰＣでの実装に依存するものであり、コンテンツプロテクションの機能が充分に強いものと言えない問題があった。すなわち、アプリケーションソフトウェアなどのリバースエンジニアリングによって、著作権保護技術に関わる秘密情報の解析により暗号方式が破られ、ディスクからのデータとしてＰＣがそのまま読み出した暗号化コンテンツが「ＤｅＣＳＳ」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を招くことで、著作権保護が機能しなくなるという危険性があった。

この発明の目的は、ＰＣ環境下でも著作権保護技術の安全性を確保することができる相互認証方法、プログラム、記録媒体、信号処理システム、再生装置および情報処理装置を提供することにある。

発明の開示

上述した課題を解決するために、この発明の第１の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達部を介して相互認証接続される情報処理装置とを備える信号処理システムであって、

再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、

中間鍵情報を伝達部を介して情報処理装置へ送る第１の送信部と、

コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第２の送信部とを有し、

情報処理装置は、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化部と、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録部とを有する信号処理システムである。

この発明の第２の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達部を介して相互認証接続される情報処理装置とが、記録媒体に情報を記録する記録方法であって、

再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

中間鍵情報を伝達部を介して情報処理装置へ送る第１の送信ステップと、

コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第2の送信ステップとを有し、

情報処理装置は、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録ステップとを有する記録方法である。

この発明の第3の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達部を介して相互認証接続される情報処理装置とが、記録媒体に情報を記録するプログラムであって、

再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

中間鍵情報を伝達部を介して情報処理装置へ送る第1の送信ステップと、

コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第2の送信ステップとを行わせ、

情報処理装置に、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記

録媒体に記録する記録ステップとを行わせるプログラムである。

この発明の第4の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、再生装置が伝達部を介して相互認証接続される情報処理装置とが、記録媒体に情報を記録するプログラムを格納した記録媒体であって、

再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

中間鍵情報を伝達部を介して情報処理装置へ送る第1の送信ステップと、

コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第2の送信ステップを行わせ、

情報処理装置に、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録ステップとを行わせるプログラムを格納した記録媒体である。

この発明の第5の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出し、伝達部を介して情報処理装置と接続される再生装置であって、　中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、

中間鍵情報を伝達部を介して情報処理装置へ送る第1の送信部と、

コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第2

の送信部とを有し、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化部と、暗号化されたコンテンツ情報および暗号化された中間鍵情報とを記録媒体に記録する記録部とを有する情報処理装置と相互認証接続される再生装置である。

この発明の第6の態様は、記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と伝達部を介して接続される情報処理装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、中間鍵情報を伝達部を介して情報処理装置へ送る第1の送信部と、コンテンツ情報暗号化鍵を伝達部を介して情報処理装置へ送る第2の送信部とを有する再生装置と伝達部を介して相互認証接続され、

コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、

記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて中間鍵情報を暗号化する中間鍵情報暗号化部と、

暗号化されたコンテンツ情報および暗号化された中間鍵情報を記録媒体に記録する記録部とを有する情報処理装置である。

この発明の第7の態様は、不正な電子機器を無効化するための第1の情報と、コンテンツ毎に異なる第2の情報と、暗号化単位毎に定義可能な第3の情報と、スタンパ毎に異なる識別データとが記録された記録媒体へ暗号化されたデータを記録する記録部および記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方

と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第4の情報が格納される格納部と、

第1の情報と第4の情報とから当該格納された第4の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であるかを判定するリボーク処理部と、

リボーク処理部で第4の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であると判定された場合に、第1の情報、第4の情報、第2の情報および識別データから、個々の記録媒体毎に固有の中間鍵情報を求める演算部と、

中間鍵情報を伝達部を介して情報処理装置の最終暗号化鍵生成部へ送る送信部とを有する再生装置である。

この発明の第8の態様は、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第4の情報を有するとともに、不正な電子機器を無効化するための第1の情報と、コンテンツ毎に異なる第2の情報と、暗号化単位毎に定義可能な第3の情報と、スタンパ毎に異なる識別データとが記録された記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置との認証を行う認証部と、

記録再生装置から、認証が成立した場合に形成されるセッションキーによって暗号化された、第1の情報、第4の情報、第2の情報および識別データから生成された個々の記録媒体毎に固有の中間鍵情報を受け取り、当該中間鍵情報を復号する鍵情報復号部と、

記録再生装置から受け取った第3の情報と、復号された中間鍵情報

から最終暗号化鍵を生成する最終暗号化鍵生成部と、

最終暗号化鍵による暗号化と最終暗号化鍵による復号との少なくとも一方を行う暗号化復号部とを有するデータ処理装置である。

この発明では、再生装置側でコンテンツキーを生成し、情報処理装置側でコンテンツキーによってコンテンツを暗号化している。このように著作権保護のための鍵情報の生成を再生装置で行うので、ハードウェア構成でコンテンツキーを生成することが可能となり、耐タンパー性を高めることができる。また、再生装置において、乱数を生成し、乱数を中間鍵とするので、再生装置において、真正乱数またはそれに近い乱数をハードウェア例えばＬＳＩによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。このように、この発明では、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

この発明では、電子機器固有の情報としてのデバイスキーを記録再生装置が持つことによって、記録再生装置自身をリボークすることが可能となる。この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばＬＳＩによって生成できるので、ＰＣ内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる等のおそれを少なくできる。

図面の簡単な説明

第１図は、先に提案されているレコーダ、プレーヤおよびＤＶＤメディアからなるシステムを説明するためのブロック図である。

第２図は、ＰＣベースのＤＶＤメディア記録再生システムを説明するためのブロック図である。

第３図は、第２図のシステムにおけるＤＶＤドライブ４およびホスト５の処理の手順を説明するための略線図である。

第４図は、第２図のシステムにおける認証動作を説明するためのフローチャートである。

第５図は、この発明の一実施形態による相互認証のための構成を示すブロック図である。

第６図は、この発明の一実施形態におけるドライブの認証動作の処理の手順を説明するためのフローチャートである。

第７図は、この発明の一実施形態におけるホストの認証動作の処理の手順を説明するためのフローチャートである。

第８図は、この発明の一実施形態によるドライブとホストを組み合わせたレコーダの構成の一例を示すブロック図である。

第９図は、レコーダの一例の通信の手順を説明するための略線図である。

第１０図は、この発明の一実施形態によるドライブとホストを組み合わせたプレーヤの構成の一例を示すブロック図である。

第１１図は、プレーヤの一例の通信の手順を説明するための略線図である。

第１２図は、この発明の他の実施形態によるドライブとホストを組み合わせたレコーダの構成の一例を示すブロック図である。

第１３図は、この発明の他の実施形態によるドライブとホストを組み合わせたプレイヤの構成の一例を示すブロック図である。

発明を実施するための最良の形態

この発明の一実施形態の説明に先立って、特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

記録媒体：メディア例えばディスク、再生装置：ドライブ、情報処理装置：ホスト、伝達手段：ドライブーホストインターフェース、信号処理システム：メディアを再生するドライブとホストとがドライブーホストインターフェースを介して接続されるシステムである。第1の送信手段：ドライブ側からセッションキーを共通鍵とした共通鍵暗号方式で情報をホスト側に送る手段、第2の送信手段：逆にホスト側からセッションキーを共通鍵として情報をドライブ側に送る手段のことである。

コンテンツ情報：メディアに記録されている情報または記録すべき情報をコンテンツ情報としている。記録媒体固有の情報：メディアＩＤである。乱数を生成する乱数生成手段：乱数発生器（ＲＮＧ：Random Number Generator)である。記録媒体固有の鍵情報：メディアユニークキー、中間鍵情報：タイトルキーである。コンテンツ情報暗号化鍵：コンテンツキー（記録時に使われるコンテンツキーをコンテンツ情報暗号化鍵とし、再生時に使われるコンテンツキーをコンテンツ情報復号鍵としている。）

この発明の理解の容易のために、最初に第1図を参照して著作権保護技術例えばＤＶＤ用ＣＰＲＭのアーキテクチャについて説明する。第1図において、参照符号1が例えばＣＰＲＭ規格に準拠したＤＶＤ－Ｒ／ＲＷ、ＤＶＤ－ＲＡＭ等の記録型ＤＶＤメディアを示す。参照符号2が例えばＣＰＲＭ規格に準拠したレコーダを示す。参照符号3

が例えばＣＰＲＭ規格に準拠したプレーヤを示す。レコーダ２およびプレーヤ３は、機器またはアプリケーションソフトウェアである。

未記録ディスクの状態において、ＤＶＤメディア１の最内周側のリードインエリアのＢＣＡ(Burst Cutting Area)またはＮＢＣＡ(Narrow Burst Cutting Area)と称されるエリアには、メディアＩＤ１１が記録されている。リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック（以下、ＭＫＢと適宜略す）１２が予め記録されている。メディアＩＤ１１は、個々のメディア単位例えばディスク１枚毎に異なる番号であり、メディアの製造者コードとシリアル番号から構成される。メディアＩＤ１１は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロックＭＫＢは、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための鍵束である。これらのメディアＩＤおよびメディアキーブロックは、記録媒体固有の第１の情報である。

ディスク１の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ１３が記録される。暗号化方式としては、Ｃ２(Cryptomeria Ciphering)が使用される。

ＤＶＤメディア１には、暗号化タイトルキー１４およびＣＣＩ(Copy Control Information)１５が記録される。暗号化タイトルキー１４は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。ＣＣＩは、コピーノーモア、コピーワンス、コピーフリー等のコピー制御情報である。

レコーダ２は、デバイスキー２１、プロセスＭＫＢ２２、Ｃ２＿Ｇ２３、乱数発生器２４、Ｃ２＿Ｅ２５、Ｃ２＿Ｇ２６およびＣ２＿ＥＣＢＣ２７の構成要素を有する。プレーヤ３は、デバイスキー３１、

プロセスＭＫＢ３２、Ｃ２＿Ｇ３３、Ｃ２＿Ｄ３５、Ｃ２＿Ｇ３６およびＣ２＿ＤＣＢＣ３７の構成要素を有する。Ｃ２＿Ｇ２３および３３は、それぞれメディアＩＤとメディアキーとからメディアユニークキーを演算するブロックである。Ｃ２＿Ｇ２６および３６は、それぞれＣＣＩとタイトルキーとからコンテンツキーを演算するブロックである。

デバイスキー２１、３１は、個々の装置メーカ、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。ＤＶＤメディア１から再生されたＭＫＢ１２とデバイスキー２１とがプロセスＭＫＢ２２において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ２におけるのと同様に、プレーヤ３においても、ＭＫＢ１２とデバイスキー３１とがプロセスＭＫＢ３２において演算され、リボケーションされたかどうかの判別がなされる。

プロセスＭＫＢ２２、３２のそれぞれにおいて、ＭＫＢ１２とデバイスキー２１、３１からメディアキーが算出される。ＭＫＢ１２の中にレコーダ２またはプレーヤ３のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ２またはプレーヤ３が正当なものでないと判断される。すなわち、そのようなレコーダ２またはプレーヤ３がリボケーションされる。

Ｃ２＿Ｇ２３、３３は、それぞれ、メディアキーとメディアＩＤとを演算し、メディアユニークキーを導出する処理である。

乱数発生器（ＲＮＧ：Random Number Generator）２４は、タイトル

キーの生成に利用される。乱数発生器２４からのタイトルキーがＣ２＿Ｅ２５に入力され、タイトルキーがメディアユニークキーで暗号化される。暗号化タイトルキー１４がＤＶＤメディア１に記録される。

プレーヤ３では、ＤＶＤメディア１から再生された暗号化タイトルキー１４とメディアユニークキーとがＣ２＿Ｄ３５に供給され、暗号化タイトルキーがメディアユニークキーで復号され、タイトルキーが得られる。

レコーダ２においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ２６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ２７に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１３がＤＶＤメディア１に記録される。

プレーヤ３においては、ＣＣＩとタイトルキーとがＣ２＿Ｇ３６に供給され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＥＣＢＣ３７に供給され、ＤＶＤメディア１から再生された暗号化コンテンツ１３がコンテンツキーを鍵として復号される。

第１図の構成において、レコーダ２による記録の手順について説明する。レコーダ２は、ＤＶＤメディア１からＭＫＢ１２を読み出し、プロセスＭＫＢ２２によってデバイスキー２１とＭＫＢ１２とを演算し、メディアキーを計算する。演算結果が予め定められた値を示すならば、デバイスキー２１（レコーダ２の機器またはアプリケーション）がＭＫＢによってリボークされたと判定される。レコーダ２は、以後の処理を中断し、ＤＶＤメディア１への記録を禁止する。若し、メディアキーの値が予め定められた値以外であれば、処理を継続する。

レコーダ２は、ＤＶＤメディア１からメディアＩＤ１１を読み、メディアキーと共にメディアＩＤをＣ２＿Ｇ２３に入力しメディア毎に異なるメディアユニークキーが演算される。乱数発生器２４で発生さ

せたタイトルキーがＣ２＿Ｅ２５で暗号化され、暗号化タイトルキー１４としてＤＶＤメディア１に記録される。タイトルキーとコンテンツのＣＣＩ情報がＣ２＿Ｇ２６で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをＣ２＿ＥＣＢＣ２７で暗号化し、ＤＶＤメディア１上に暗号化コンテンツ１３としてＣＣＩ１５と共に記録する。

プレーヤ３による再生の手順について説明する。最初にＭＫＢ１２をＤＶＤメディア１から読み出す。デバイスキー３１とＭＫＢ１２を演算し、リボケーションの確認がなされる。デバイスキー３１、すなわち、プレーヤ３の機器またはアプリケーションがリボークされない場合には、メディアＩＤを使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー１４とメディアユニークキーからタイトルキーが演算される。タイトルキーとＣＣＩ１５とがＣ２＿Ｇ３６に入力され、コンテンツキーが導出される。コンテンツキーがＣ２＿ＤＣＢＣ３７に入力され、コンテンツキーを鍵として、ＤＶＤメディア１から再生された暗号化コンテンツ１３に対してＣ２＿ＤＣＢＣ３７の演算が施される。その結果、暗号化コンテンツ１３が復号される。

このように、コンテンツの復号に必要なコンテンツキーを得るためには、ＤＶＤメディアの１枚毎に異なるメディアＩＤが必要となるので、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディアＩＤがオリジナルのメディアＩＤと異なるために、コピーされたコンテンツを復号することができず、コンテンツの著作権を保護することができる。

上述した第１図の構成は、記録再生機器として構成されたものである。この発明は、ＤＶＤメディア１に対するコンテンツ保護処理をＰ

C環境下で扱う場合に適用される。第2図を参照して現行の方式によるＰＣとドライブの役割分担を示す。第2図において、参照符号4が上述したＣＰＲＭ規格に準拠したＤＶＤメディア1を記録および再生する記録再生装置としてのＤＶＤドライブを示す。

参照符号5がデータ処理装置としてのホスト例えばＰＣを示す。ホスト5は、ＤＶＤメディア1に記録可能で、ＤＶＤメディア1から再生可能なコンテンツを扱うことができ、且つＤＶＤドライブ4と接続されてデータ交換が可能な装置またはアプリケーションソフトウェアである。例えばＰＣに対してアプリケーションソフトウェアがインストールされることによってホスト5が構成される。

ＤＶＤドライブ4とホスト5との間がインターフェース4ａで接続されている。インターフェース4ａは、ＡＴＡＰＩ(AT Attachment with Packet Interface)，ＳＣＳＩ(Small Computer System Interface)，ＵＳＢ(Universal Serial Bus)，ＩＥＥＥ(Institute of Electrical and Electronics Engineers) 1394等である。

ＤＶＤメディア1には、メディアＩＤ11、メディアキーブロック12およびＡＣＣ(Authentication Control Code) が予め記録されている。ＡＣＣは、ＤＶＤドライブ4とホスト5との間の認証がＤＶＤメディア1によって異なるようにするために予めＤＶＤメディア1に記録されたデータである。

ＤＶＤドライブ4は、ＡＣＣ16をＤＶＤメディア1から読み出す。ＤＶＤメディア1から読み出されたＡＣＣ16がＤＶＤドライブ4のＡＫＥ(Authentication and Key Exchange) 41に入力されると共に、ホスト5へ転送される。ホスト5は、受け取ったＡＣＣをＡＫＥ51に入力する。ＡＫＥ41および51は、乱数データを交換し、この交換した乱数とＡＣＣの値とから認証動作の度に異なる値となる共

通のセッションキー（第２図の構成においてはバスキーと称する）を生成する。

バスキーがＭＡＣ(Message Authentication Code) 演算ブロック４２および５２にそれぞれ供給される。ＭＡＣ演算ブロック４２および５２は、ＡＫＥ４１および５１でそれぞれ得られたバスキーをパラメータとして、メディアＩＤおよびメディアキーブロック１２のＭＡＣを計算するプロセスである。ＭＫＢとメディアＩＤの完全性(integrity) をホスト５が確認するために利用される。

ＭＡＣ４２および５２によってそれぞれ計算されたＭＡＣがホスト５の比較５３において比較され、両者の値が一致するかどうかが判定される。これらのＭＡＣの値が一致すれば、ＭＫＢとメディアＩＤの完全性が確認されたことになる。比較出力でスイッチＳＷ１が制御される。

スイッチＳＷ１は、ＤＶＤドライブ４のＤＶＤメディア１の記録または再生経路と、ホスト５の暗号化／（または）復号モジュール５４との間の信号路をＯＮ／ＯＦＦするものとして示されている。スイッチＳＷ１は、信号路のＯＮ／ＯＦＦを行うものとして示されているが、より実際には、ＯＮの場合にホスト５の処理が継続し、ＯＦＦの場合にホスト５の処理が停止することを表している。暗号化／復号モジュール５４は、メディアユニークキーと暗号化タイトルキーとＣＣＩとからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ１３へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ１３を復号する演算ブロックである。

メディアユニークキー演算ブロック５５は、ＭＫＢ１２とメディアＩＤとデバイスキー５６とからメディアユニークキーを演算する演算ブロックである。第１図に示すレコーダまたはプレーヤと同様に、デ

バイスキーとＭＫＢ１２とからメディアキーが演算される。メディアキーとメディアＩＤ１１とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボークされる。したがって、メディアユニークキー演算ブロック５５は、リボケーションを行うリボーク処理部としての機能も有する。

記録時に、比較５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされる。暗号化／復号モジュール５４からスイッチＳＷ１を通じてドライブ４に対して、暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５が供給され、ＤＶＤメディア１に対してそれぞれ記録される。再生時に、比較５３によって完全性が確認された場合には、スイッチＳＷ１がＯＮされる。ＤＶＤメディア１からそれぞれ再生された暗号化コンテンツ１３、暗号化タイトルキー１４およびＣＣＩ１５がスイッチＳＷ１を通じてホスト５の暗号化／復号モジュール５４に対して供給され、暗号化コンテンツが復号される。

第３図は、第２図に示す現行のＰＣ環境下のＤＶＤメディアを利用するシステムにおいて、ＤＶＤメディア１と、ＤＶＤドライブ４と、ホスト５との間の信号の授受の手順を示す。ホスト５がＤＶＤドライブ４に対してコマンドを送り、ＤＶＤドライブ４がコマンドに応答した動作を行う。

ホスト５からの要求に応じてＤＶＤメディア１上のＡＣＣがシークされ、読み出される（ステップＳ１）。次のステップＳ２において、読み出されたＡＣＣがＡＫＥ４１に入力されると共に、ホスト５へ転送され、ホスト５では、受け取ったＡＣＣがＡＫＥ５１へ入力される。ＡＫＥ４１および５１は、乱数データを交換し、この交換した乱数

とＡＣＣ１６の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーをＤＶＤドライブ４とホスト５が共有する。相互認証が成立しなかった場合では、処理が中断する。

認証動作は、電源のＯＮ後のディスク検出時並びにディスクの交換時には、必ず行われる。記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

認証が成功すると、ステップＳ３において、ホスト５がＤＶＤドライブ４に対して、ＤＶＤメディア１からのＭＫＢ（メディアキーブロック）パック＃０の読み出しを要求する。ＭＫＢは、パック０～パック１５の１６セクタが１２回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

ＤＶＤドライブ４がステップＳ４においてＭＫＢのパック＃０を読みに行き、ステップＳ５において、パック＃０が読み出される。ＤＶＤドライブ４は、モディフアイドＭＫＢをホスト５へ戻す（ステップＳ６）。ＭＫＢを読み出す際に、バスキーをパラメータとしてＭＡＣ値を計算し、ＭＫＢに対してＭＡＣ値を付加してホスト５へデータを転送する。パック＃０以外の残りのＭＫＢパックの要求と、ＤＶＤドライブ４の読み出し動作と、モディフアイドＭＫＢパックの転送動作とがＭＫＢのパックがなくなるまで、例えばパック＃１５が読み出され、ホスト５へ転送されるまで、ステップＳ７およびＳ８によって繰り返しなされる。

ホスト５がＤＶＤドライブ４に対してメディアＩＤを要求する。ＤＶＤドライブ４がＤＶＤメディア１に記録されているメディアＩＤを読みに行き、ステップＳ１１において、メディアＩＤが読み出される

。ＤＶＤドライブ４は、メディアＩＤを読み出す際に、バスキーをパラメータとしてそのＭＡＣ値を計算する。ＤＶＤドライブ４はステップＳ１２において、読み出されたメディアＩＤに対してＭＡＣ値ｍ１を付加してホスト５へデータを転送する。

ホスト５では、ＤＶＤドライブ４から受け取ったＭＫＢ１２およびメディアＩＤ１１からバスキーをパラメータとして再度ＭＡＣ値を計算し、計算したＭＡＣ値とＤＶＤドライブ４から受け取ったＭＡＣ値とを比較５３で比較する。両者が一致したならば、正しいＭＫＢおよびメディアＩＤを受け取ったと判定して、スイッチＳＷ１をＯＮに設定して処理を先に進める。逆に両者が一致しなかったならば、ＭＫＢおよびメディアＩＤが改ざんされたものと判定して、スイッチＳＷ１をＯＦＦに設定して処理を中断する。

ステップＳ１３において、ホスト５がＤＶＤドライブ４に対して暗号化コンテンツを要求し、ステップＳ１４において、ＤＶＤドライブ４が暗号化コンテンツを読み出し、ステップＳ１３において、読み出した暗号化コンテンツがホスト５に転送される。ホスト５のメディアユニークキー演算ブロック５５では、デバイスキー５６とＭＫＢ１２とメディアＩＤ１１とによってメディアユニークキーが計算される。メディアユニークキーが暗号化／復号モジュール５４に供給され、暗号化タイトルキー１４、ＣＣＩ１５からコンテンツキーが求められる。コンテンツキーを鍵としてＤＶＤメディア１から読み出された暗号化コンテンツが復号される。ＤＶＤメディア１に対して記録されるコンテンツが暗号化される。

第４図のフローチャートにおいて、ステップＳＴ１は、ＭＡＣ演算ブロック４２でバスキーをパラメータとして求められたＭＡＣ計算値と、ＭＡＣ演算ブロック５３でバスキーをパラメータとして求められ

たＭＡＣ計算値とを比較するステップである。両者が一致すれば、スイッチＳＷ１がステップＳＴ２においてＯＮとされる。両者が一致しない場合では、スイッチＳＷ１がステップＳＴ３においてＯＦＦとされ、処理が停止する。

上述したＣＰＲＭでは、ＤＶＤ－Video の著作権保護技術であるＣＳＳと同じバスキー生成方法を採用している。ＣＳＳ認証方式の内容は、本来秘密であるべき情報であるが、既に解析され一般ユーザーが入手可能なＣＳＳライセンス管理団体であるＤＶＤ－ＣＣＡの許諾を得ていないフリーソフトウェアによって動作させることが可能となっている。加えて、コンテンツプロテクション処理は、ホスト側でなされる、すなわち、リボケーション判定、メディアキー取得、メディアユニークキー導出、タイトルキー生成・導出からコンテンツキー導出およびコンテンツ暗号化・復号の全てがホスト側の処理であることから、著作権保護技術としての信頼性が低下している。

以下に述べるこの発明の一実施形態では、かかる問題点を解決するものである。一実施形態では、ＰＣ環境下でのコンテンツプロテクション処理におけるタイトルキー導出に関わる構成をドライブ内部に持ち、ＰＣとの相互認証を経てタイトルキーおよびコンテンツキーをＰＣに送信するものである。

第５図は、一実施形態における相互認証の構成を示すブロック図であり、第６図は、ドライブ側の処理の流れを示すフローチャートであり、第７図は、ホスト側の処理の流れを示すフローチャートである。以下の説明において、参照符号１０１がメディア例えば光ディスクを示し、参照符号１０２がメディアのドライブを示し、参照符号１０３がドライブ１０２とドライブーホストインターフェース１０４を介して接続されたホストを示す。メディア１０１は、上述したＤＶＤメデ

ィアと同様の情報が予め記録されているものである。メディア１０１は、記録可能なものに限らず、読み出し専用のものでも良い。ホスト１０３がドライブ１０２に対して所定のコマンドを送り、その動作を制御する。使用するコマンドは、上述した非特許文献２に記載されているコマンド並びにコマンドを拡張したもの、および、メディア１０１からコンテンツをセクタ・データとして読み出すためのＲＥＡＤコマンド、メディア１０１へコンテンツをセクタ・データとして書き込むためのＷＲＩＴＥコマンドである。

ドライブ１０２は、ドライブのデバイスキー１２１を有し、ホスト１０３がホストのデバイスキー１３１を有している。デバイスキー１２１は、多くの場合にＬＳＩ(Large Scale Integrated Circuit ：大規模集積回路）内部に配置され、外部から読み出すことができないようセキュアに記憶される。デバイスキー１３１は、ソフトウェアプログラム内にセキュアに記憶される場合と、ハードウェアとしてセキュアに記憶される場合とがある。ドライブ１０２がメディア１０１を扱う正当なドライブとなるためには、一実施形態のように、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

第５図に示すように、ドライブ１０２には、ＭＫＢとデバイスキー１２１とが入力され、ドライブのデバイスキーがリボケーションされたかどうかを判定するプロセスＭＫＢ１２２が備えられている。ホスト１０３にも同様に、プロセスＭＫＢ１３２が備えられている。リボケーションされない場合に、プロセスＭＫＢ１２２および１３２からそれぞれメディアキーＫｍが出力される。リボーク判定処理がなされ、メディアキーＫｍが得られてから認証処理がなされる。

参照符号１２３、１２４および１２５は、メディアキーＫｍをパラメータとしてＭＡＣ値を計算するＭＡＣ演算ブロックをそれぞれ示す。参照符号１２６、１２７および１２８は、乱数発生器（ＲＮＧ：Random Number Generator ）をそれぞれ示す。乱数発生器１２６が乱数Ra1を生成し、乱数発生器１２７が乱数Ra2を生成し、乱数発生器１２８が乱数Ra3を生成する。乱数発生器１２６、１２７、１２８は、例えばＬＳＩの構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を共通のハードウェアとしても良いが、乱数Ra1、Ra2、Ra3は、互いに独立したものである。

ホスト１０３に、メディアキーＫｍをパラメータとしてＭＡＣ値を計算するＭＡＣ演算ブロック１３３、１３４および１３５と、乱数発生器１３６、１３７および１３８が備えられている。乱数発生器１３６が乱数Rb1を生成し、乱数発生器１３７が乱数Rb2を生成し、乱数発生器１３８が乱数Rb3を生成する。乱数発生器１３６、１３７、１３８は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェアによる乱数が利用できる場合にはこれを用いても良い。

ドライブ１０２において生成された乱数とホスト１０３において生成された乱数とが交換される。すなわち、乱数Ra1および乱数Rb1がＭＡＣ演算ブロック１２３および１３３に入力され、乱数Ra2および乱数Rb2がＭＡＣ演算ブロック１２４および１３４に入力され、乱数Ra3および乱数Rb3がＭＡＣ演算ブロック１２５および１３５に入力される。

ドライブ１０２のＭＡＣ演算ブロック１２３が演算したＭＡＣ値と、ホスト１０３のＭＡＣ演算ブロック１３３が演算したＭＡＣ値とがホスト１０３内の比較１３９において比較され、二つの値が同一か否

かが判定される。ここでのＭＡＣ値は、eKm(Ral‖Rbl) と表記される。ｅＫｍ（）は、メディアキーＫｍを鍵として括弧内のデータを暗号化することを表している。Ｒａｌ‖Ｒｂｌの記号は、左側に乱数Ｒａｌを配し、右側に乱数Ｒｂｌを配するように、二つの乱数を結合することを表している。比較の結果、二つの値が同一と判定されると、ホスト１０３によるドライブ１０２の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

ホスト１０３のＭＡＣ演算ブロック１３４が演算したＭＡＣ値と、ドライブ１０２のＭＡＣ演算ブロック１２４が演算したＭＡＣ値とがドライブ１０２内の比較１２９において比較され、二つの値が同一か否かが判定される。ここでのＭＡＣ値は、eKm(Rb2‖Ra2)と表記される。比較の結果、二つの値が同一と判定されると、ドライブ１０２によるホスト１０３の認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

かかる相互認証において、比較１３９および１２９の両者において、ＭＡＣ値が同一と判定され、ドライブ１０２およびホスト１０３の両者の正当性が確認されると、すなわち、相互認証が成功すると、ＭＡＣ演算ブロック１２５および１３５によって、共通のセッションキーeKm(Ra3‖Rb3)がそれぞれ生成される。

さらに、上述した相互認証の処理の流れを第６図および第７図のフローチャートを参照して説明する。最初に、第７図のステップＳＴ２０において、ホスト１０３がドライブ１０２に対して、コマンドREPORT KEYを発行し、ＭＫＢの転送を要求する。第６図のステップＳＴ１０において、ドライブ１０２がメディア１０１からＭＫＢ１１２を読み出して、ホスト１０３へ転送する。

次に、ドライブ１０２がステップＳＴ１１において、プロセスＭＫ

Ｂ１２２によってメディアキーＫｍを計算し、ホスト１０３がステップＳＴ２１において、プロセスＭＫＢ１３２によってメディアキーＫｍを計算する。この計算の過程でそれぞれが内蔵するデバイスキー１２１および１３１がリボケーションの対象とされているか否かが自分自身によって確認される（第６図中のステップＳＴ１２、第７図中のステップＳＴ２２）。

ドライブ１０２およびホスト１０３のそれぞれは、リボケーションの対象とされている場合にはリボークされ、処理が終了する。若し、ホスト１０３がリボケーションの対象とされていなければ、ステップＳＴ２３において、コマンドSEND KEYにより、ドライブ１０２に対して乱数発生器１３６および１３７でそれぞれ生成された乱数Ｒb1と乱数Ｒb2を転送する。若し、ドライブ１０２がリボケーションの対象とされていなければ、ステップＳＴ１３において、ドライブ１０２がホスト１０３から転送されたこれらの乱数を受け取る。

その後、ホスト１０３は、コマンドREPORT KEYによりドライブ１０２に対してドライブ１０２が持つメディアキーＫｍを鍵としたＭＡＣによるレスポンス値と乱数生成器１２６が発生した乱数Ralとをホスト１０３へ転送することを要求する（ステップＳＴ２４）。このレスポンス値は、eKm(Ral‖Rbl)と表記される。ｅＫｍ（）は、メディアキーＫｍを暗号鍵として括弧内のデータを暗号化することを表している。Ral‖Rblの記号は、左側に乱数Ralを配し、右側に乱数Rblを配するように、二つの乱数を結合することを表している。

ホスト１０３からコマンドREPORT KEYを受け取ったドライブ１０２は、ステップＳＴ１４において、ＭＡＣ演算ブロック１２３が生成したＭＡＣ値eKm(Ral‖Rbl)と乱数Ralをホスト１０３へ転送する。ステップＳＴ２５において、ホスト１０３は、自身のＭＡＣ演算ブロッ

ク１３３でＭＡＣ値を計算し、比較１３９においてドライブ１０２から受け取った値と一致するかの確認を行う。若し、受け取ったＭＡＣ値と計算されたＭＡＣ値とが一致したのなら、ホスト１０３によるドライブ１０２の認証が成功したことになる。ステップＳＴ２５における比較の結果が同一でない場合には、ホスト１０３によるドライブ１０２の認証が失敗したことになり、リジェクト処理がなされる。

ホスト１０３によるドライブ１０２の認証が成功した場合には、ステップＳＴ２６において、ホスト１０３がドライブ１０２へコマンドREPORT KEYを送付し、ドライブ１０２の乱数生成器１２４および１２５がそれぞれ生成する乱数Ｒa2と乱数Ｒa3の転送を要求する。このコマンドに応答して、ステップＳＴ１５において、ドライブ１０２は、これらの乱数をホスト１０３へ転送する。

ステップＳＴ２７において、ホスト１０３のＭＡＣ演算ブロック１３４は、ドライブ１０２から受け取った乱数からホスト１０３が持つメディアキーＫｍを鍵としたＭＡＣによるレスポンス値eKm(Rb2‖Ra2)を計算し、乱数Ｒb3とともに、コマンドSEND KEYを用いてドライブ１０２へ転送する。

ステップＳＴ１６において、ドライブ１０２は、ホスト１０３からレスポンス値eKm(Rb2‖Ra2)および乱数Rb3 を受け取ると、自身でＭＡＣ値を計算し、ステップＳＴ１７において、比較１２９によってホスト１０３から受け取ったＭＡＣ値と一致するかの確認を行う。若し、受け取ったＭＡＣ値と計算されたＭＡＣ値とが一致したのなら、ドライブ１０２によるホスト１０３の認証が成功したことになる。この場合には、ステップＳＴ１８において、ＭＡＣ演算ブロック１２５がセッションキーeKm(Rb3‖Ra3)を生成し、ホスト１０３に対して認証が成功したことを示す情報を送信し、認証処理が完了する。セッショ

ンキーは、認証動作の度に異なる値となる。

ステップＳＴ１７における比較の結果が同一でない場合には、ドライブ１０２によるホスト１０３の認証が失敗したことになり、ステップＳＴ１９において、認証が失敗したことを示すエラー情報がホスト１０３に送信される。

ホスト１０３は、送付したコマンドSEND KEYに対する応答としてドライブ１０２から認証が成功したか否かを示す情報を受け取り、受け取った情報に基づいてステップＳＴ２８において、認証完了か否かを判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステップＳＴ２９において、ＭＡＣ演算ブロック１３５がドライブ側と共通のセッションキーeKm(Ra3‖Rb3)（例えば６４ビット長）を生成する。認証が完了しなかった場合には、リジェクト処理がなされる。セッションキーeKm(Ra3‖Rb3)を以下の説明では、適宜Ｋｓと表記する。

上述した一実施形態による相互認証は、ドライブ１０２がリボケーション機能を持つことができ、認証専用の特定の認証鍵を必要としない特徴を有している。

さらに、ドライブ１０２が比較１２９によってホスト１０３の認証結果を確認することで、ドライブ１０２がホスト１０３から正規のライセンスを受けた上で実装されたものであるか否かを判定することが可能となる。

次に、上述した相互認証を行うドライブ１０２とホスト１０３とを組み合わせて実現したレコーダの一実施形態の構成を第８図に示す。一実施形態のレコーダは、ドライブ１０２が計算したメディアユニークキーを相互認証によって生成したセッションキーＫｓを用いてセキ

ュアにホスト１０３に転送する。また、ドライブ１０２の乱数発生器１４３によってタイトルキーが生成される。ドライブ１０２においてタイトルキーおよびＣＣＩ２３２からコンテンツキーが生成され、生成されたコンテンツキーがセッションキーＫｓを用いてホスト１０３へセキュアに転送され、ホスト１０３が復号したコンテンツキーを用いてコンテンツを暗号化し、暗号化コンテンツをドライブ１０２へ転送し、ドライブ１０２が暗号化コンテンツ、暗号化タイトルキーおよびＣＣＩ２３２をメディア１０１へ記録する構成とされている。メディア１０１に記録されているＣＣＩに対して参照符号１１５を付す。すなわち、ドライブ１０２において、メディアユニークキーおよびコンテンツキーを生成している。

レコーダを構成するドライブ１０２は、デバイスキー１２１、プロセスＭＫＢ１２２、Ｃ２＿Ｇ２１４１、ＤＥＳ(Data Encryption Standard)エンクリプタ１４２、乱数発生器１４３、Ｃ２＿Ｇ１４５、ＤＥＳエンクリプタ１４６の構成要素を有する。Ｃ２＿Ｇ２１４１は、メディアＩＤとメディアキーからメディアユニークキーを演算するブロックである。Ｃ２＿Ｇ２１４５は、タイトルキーとＣＣＩ２３２とからコンテンツキーを演算するブロックである。

メディア１０１から再生されたＭＫＢ１１２とデバイスキー１２１とがプロセスＭＫＢ１２２において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスＭＫＢ１２２において、ＭＫＢ１１２とデバイスキー１２１からメディアキーが算出される。ＭＫＢ１１２の中にドライブ１０２のデバイスキー１２１が入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキー１２１を持つドライブ１０２が正当なものでないと判断され、ドライブ１０２がリボケーションされる

。

Ｃ２＿Ｇ１４１は、メディアキーとメディアＩＤ１１１とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがＤＥＳエンクリプタ１４２にてセッションキーＫｓによって暗号化される。暗号化の方式として、例えばＤＥＳ　ＣＢＣモードが使用される。ＤＥＳエンクリプタ１４２の出力がホスト１０３のＤＥＳデクリプタ１５１に送信される。

ドライブ１０２の乱数発生器１４３によってタイトルキーが生成され、乱数発生器１４３からのタイトルキーがホスト１０３のＣ２＿Ｅ１５３に供給され、タイトルキーがメディアユニークキーを使用してＣ２によって暗号化される。暗号化タイトルキー１１４がメディア１０１に記録される。

ホスト１０３において、セッションキーＫｓを鍵としてＭＡＣ演算ブロック１５８によりＣＣＩのＭＡＣ値ｅＫｓ（ＣＣＩ）が計算され、ＣＣＩ２３２とともにドライブ１０２へ転送される。

ドライブ１０２において、ホスト１０３から受け取ったＣＣＩ２３２からセッションキーＫｓを鍵としてＭＡＣ演算ブロック１５７によりＣＣＩのＭＡＣ値ｅＫｓ（ＣＣＩ）が計算され、ホスト１０３から受け取ったＭＡＣ値とともに比較１５９へ供給される。

比較１５９では、両方のＭＡＣ値が一致したならば、ホスト１０３から受け取ったＣＣＩ２３２の改ざんは無いものと判断し、スイッチＳＷ２をＯＮする。一致しなかった場合は、ＣＣＩは改ざんされたものとみなし、スイッチＳＷ２をＯＦＦし、以降の処理を中断する。

ドライブ１０２において、ホスト１０３から受け取ったＣＣＩ２３２とタイトルキーとがＣ２＿Ｇ１４５に供給され、コンテンツキーが導出される。コンテンツキーがＤＥＳエンクリプタ１４６に供給され

、セッションキーＫｓを鍵として、コンテンツキーが暗号化される。暗号化コンテンツキーがホスト１０３のＤＥＳデクリプタ１５６に転送される。

ホスト１０３のＤＥＳデクリプタ１５６でセッションキーＫｓを鍵として復号されたコンテンツキーがＣ２＿ＥＣＢＣ１５５に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ１１３がドライブ１０２に転送され、ドライブ１０２によってメディア１０１に記録される。

第９図は、レコーダの一実施形態によるコンテンツ記録時の手順を示すものである。最初に、ホスト１０３からの要求に応じてメディア１０１上のＭＫＢがシークされ、読み出される（ステップＳ６１）。次のステップＳ６２のＡＫＥ(Authentication and Key Exchange) において、上述したようなリボーク処理とドライブ１０２とホスト１０３の相互認証動作がなされる。

相互認証動作は、電源のＯＮ後のディスク検出時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ１０２およびホスト１０３の両者において、セッションキーＫｓが生成され、セッションキーＫｓが共有される。

次のステップＳ６３において、ホスト１０３がドライブ１０２に対してメディアユニークキーを要求する。ドライブ１０２は、メディア１０１のメディアＩＤをシークし（ステップＳ６４）、メディアＩＤ

をメディア１０１から読み出す（ステップＳ６５）。ドライブ１０２は、メディアキーとメディアＩＤとを演算することによってメディアユニークキーを生成する。ステップＳ６６において、メディアユニークキーがセッションキーＫｓによって暗号化され、暗号化されたメディアユニークキーがホスト１０３に転送される。

次に、ステップＳ６７において、ホスト１０３がドライブ１０２に対してタイトルキーを要求する。ステップＳ６８において、ドライブ１０２がタイトルキーをホスト１０３に転送する。ホスト１０３において、セッションキーＫｓによって、暗号化されたメディアユニークキーが復号される。そして、タイトルキーがメディアユニークキーによって暗号化され、暗号化タイトルキーが生成される。

また、ステップＳ６９において、ホスト１０３がドライブ１０２に対してＣＣＩ２３２を送る。このとき、ＣＣＩ２３２の改ざんを回避するためにＣＣＩ２３２の認証データとして計算されたＭＡＣ値ｅＫｓ（ＣＣＩ）を付加して転送する。ドライブ１０２において、ＣＣＩ２３２の改ざんが無いことを確認後、タイトルキーとＣＣＩ２３２からコンテンツキーが生成され、コンテンツキーがセッションキーＫｓで暗号化される。ステップＳ７０において、ホスト１０３がドライブ１０２に対してコンテンツキーを要求すると、ステップＳ７１において、ドライブ１０２が暗号化されたコンテンツキーをホスト１０３に送る。

ホスト１０３は、暗号化コンテンツキーをセッションキーＫｓによって復号し、コンテンツキーを得る。コンテンツキーによってコンテンツが暗号化される。ステップＳ７２において、ホスト１０３からドライブ１０２に対して、暗号化タイトルキー、暗号化コンテンツおよびＣＣＩ２３２が転送される。ステップＳ７３において、ドライブ１

０２によって、暗号化タイトルキー、暗号化コンテンツおよびＣＣＩ２３２がメディア１０１に対して記録される。

上述した第８図に示す構成のレコーダは、ドライブ１０２において、真正乱数またはそれに近い乱数をハードウェア例えばＬＳＩによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。また、ドライブ１０２において、ハードウェア構成によってコンテンツキーを生成するので、著作権保護の実装を強力とすることができる。

次に、上述した相互認証を行うドライブ１０２とホスト１０３とを組み合わせて実現したプレーヤの一実施形態の構成を第１０図に示す。一実施形態のプレーヤは、ドライブ１０２が計算したメディアユニークキーを相互認証によって生成したセッションキーＫｓを用いてセキュアにホスト１０３に転送し、ホスト１０３が暗号化タイトルキーをメディアユニークキーによって復号し、タイトルキーとＣＣＩ１１５とから導出したコンテンツキーを用いてコンテンツを復号する構成とされている。

プレーヤを構成するドライブ１０２は、デバイスキー１２１、プロセスＭＫＢ１２２、Ｃ２＿Ｇ２１４１、ＤＥＳエンクリプタ１４２の構成要素を有する。メディア１０１から再生されたＭＫＢ１１２とデバイスキー１２１とがプロセスＭＫＢ１２２において演算されることによって、リボケーションされたかどうかの判別ができる。プロセスＭＫＢ１２２において、ＭＫＢ１１２とデバイスキー１２１からメディアキーが算出される。

Ｃ２＿Ｇ１４１は、メディアキーとメディアＩＤ１１１とを演算し、メディアユニークキーを導出する処理である。メディアユニークキーがＤＥＳエンクリプタ１４２にてセッションキーＫｓによって暗号

化される。暗号化の方式として、例えばＤＥＳ　ＣＢＣモードが使用される。ＤＥＳエンクリプタ１４２の出力がホスト１０３のＤＥＳデクリプタ１５１に送信される。

ホスト１０３において、ＤＥＳデクリプタ１５１において、セッションキーＫｓによってメディアユニークキーが復号される。メディアユニークキーおよび暗号化タイトルキー１１４がＣ２＿Ｄ１５３に供給され、暗号化タイトルキーがメディアユニークキーを使用して復号される。復号されたタイトルキーとメディア１０１から再生されたＣＣＩ１１５がＣ２＿Ｇ１５４に供給され、コンテンツキーが導出される。メディア１０１から再生された暗号化コンテンツ１１３がＣ２デクリプタ１５５において、コンテンツキーによって復号され、コンテンツキーが得られる。

第１１図は、コンテンツ再生時の手順を示すものである。最初に、ホスト１０３からの要求に応じてメディア１０１上のＭＫＢがシークされ、読み出される（ステップＳ４１）。ＭＫＢがパック毎に読み出される。次のステップＳ４２のＡＫＥにおいて、上述したようなリボーク処理と、ドライブ１０２とホスト１０３の相互認証動作がなされる。

相互認証が成功しないと、リジェクト処理によって例えば処理が中断する。相互認証が成功すると、ドライブ１０２およびホスト１０３の両者において、セッションキーＫｓが生成され、セッションキーＫｓが共有される。

次のステップＳ４３において、ホスト１０３がドライブ１０２に対してメディアユニークキーを要求する。ドライブ１０２は、メディア１０１のメディアＩＤをシークし（ステップＳ４４）、メディアＩＤをメディア１０１から読み出す（ステップＳ４５）。ドライブ１０２

は、メディアキーとメディアＩＤとを演算することによってメディアユニークキーを生成する。ステップＳ４６において、メディアユニークキーがセッションキーＫｓによって暗号化され、暗号化されたメディアユニークキーがホスト１０３に転送される。

次に、ステップＳ４７において、ホスト１０３がドライブ１０２に対して、暗号化タイトルキー、ＣＣＩおよび暗号化コンテンツを要求する。ステップＳ４８において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３をメディア１０１からリードする。ステップＳ４９において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３を読み取る。そして、ステップＳ５０において、ドライブ１０２が暗号化タイトルキー１１４、ＣＣＩ１１５および暗号化コンテンツ１１３をホスト１０３に対して転送する。

ホスト１０３において、タイトルキーが復号され、タイトルキーとＣＣＩ１１５とからコンテンツキーが求められ、コンテンツキーを鍵として暗号化コンテンツが復号される。

第１０図に示すプレーヤの構成においては、ホスト１０３が暗号化タイトルキーを復号するデクリプタＣ２＿Ｄ１５３を備えているが、ドライブ１０２が暗号化タイトルキーを復号するデクリプタを備えるようにしても良い。この場合、復号されたタイトルキーがホスト１０３のコンテンツキー生成用のＣ２＿Ｇ１５４に対してセキュアに転送される。または、ドライブ１０２にコンテンツキー生成装置Ｃ２＿Ｇを設け、ドライブ１０２において復号されたタイトルキーとＣＣＩとからコンテンツキーを生成するようにしても良い。この場合、復号されたコンテンツキーがホスト１０３のＣ２＿ＤＣＢＣ１５５へセキュアに転送される。

この発明のレコーダおよびプレイヤの他の実施形態について、第１２図および第１３図を参照して説明する。他の実施形態は、メディアユニークキーをドライブで生成するものであり、コンテンツキーを生成する場合に関与するパラメータを使用するもの（ＣＰＲＭを拡張したシステム）である。

ＣＰＲＭを拡張したシステムにおいて、メディアユニークキーを演算するためのパラメータＡと、暗号化／復号のためのパラメータＢとが使用される。これらのパラメータＡ，Ｂがホスト側にある場合と、ドライブ側にある場合と、メディアに記録されており、ホストが読み出す場合との全てが可能である。パラメータＡ，Ｂをインターフェースを介して授受する場合には、暗号化を行い、セキュアに伝送しても良い。

第１２図は、レコーダの他の実施形態の構成を示す。第１２図において、参照符号２０１が記録可能なメディアを示し、メディア２０１には、ＥＫＢ２１１、暗号化ディスクキーＥｍ（Ｋｄ）２１２、ディスクＩＤ２１３およびユニットキー生成用値Ｖｕ２１４が記録されている。

第１２図中に記載されている鍵情報に関する用語を下記に説明する。

ＥＫＢ２１１は、各デバイスキーに対してメディアキーＫｍを配布するための鍵束である。既述の実施形態におけるメディアキーブロックＭＫＢに相当する。

メディアキーＫｍは、メディア毎に固有の鍵情報である。ＥＫＢの中にメディアキーが見つからない場合は、そのデバイスキーがリボークされたことを示す。

ディスクキーＫｄは、少なくともコンテンツ毎に異なる鍵情報であ

る。コンテンツのマスターディスク毎に異ならせても良い。暗号化ディスクキーＥｍ（Ｋｄ）２１２は、メディアキーＫｍでディスクキーＫｄを暗号化した暗号化鍵で、メディア２０１に記録されている。暗号化ディスクキーＥｍ（Ｋｄ）２１２は、ドライブ１０２において、個々のメディア毎に異なるエンベディッドキーＫｅを生成するために使用される。

ユニットキー生成用値Ｖｕ２１４は、暗号化単位（暗号化ユニットと称する）ごとに定義することが可能なパラメータである。各暗号化ユニットは、複数のセクタデータから構成される。ユニットキー生成用値Ｖｕ２１４は、ホスト１０３においてコンテンツを暗号化する暗号化鍵としてのユニットキーＫｕを生成するために使用される。

ディスクＩＤ２１３は、スタンパ毎に異なるＩＤである。一実施形態におけるメディアＩＤ１１１に相当する。

エンベディッドキーＫｅは、個々のメディア毎に異なる鍵情報であり、一実施形態におけるメディアユニークキーに相当する。

ドライブ１０２が持つデバイスキー２２１と、メディア２０１が持つＥＫＢ２１１とに基づいてプロセスＥＫＢ２２２によってメディアキーＫｍが得られる。メディアキーＫｍとメディア２０１が持つ暗号化ディスクキーＥｍ（Ｋｄ）２１２とに基づいてＡＥＳ＿Ｄ２２３においてディスクキーＫｄが復号される。ディスクキーＫｄとディスクＩＤ２１３とに基づいてＡＥＳ＿Ｇ２２４においてエンベディッドキーＫｅが得られる。

ユニットキーＫｕは、コンテンツを暗号化する鍵であり、エンベディッドキーＫｅとユニットキー生成用値Ｖｕとコピー制御情報ＣＣＩ２３２とに基づいて得られる。ユニットキーＫｕは、上述の一実施形態におけるコンテンツキーに相当する。

上述した他の実施形態のレコーダの動作について処理の流れにしたがって説明する。

最初にＡＫＥ２２５および２２７による認証がなされる。認証が成功すると、セッションキーＫｓが生成される。第１２図では省略されているが、ＡＫＥ２２５および２２７の少なくとも一方に対して認証に関係するパラメータが供給されている。

ドライブ１０２は、メディア２０１からＥＫＢ２１１を読み出す。メディア２０１からのＥＫＢ２１１とデバイスキー２２１がドライブ１０２のプロセスＥＫＢ２２２で演算され、メディアキーＫｍが算出される。演算結果が例えば０になるような場合では、デバイスキーがリボークされる。ドライブ１０２が有しているデバイスキー２２１は、例えば機種単位でドライブに与えられる固有の鍵である。

ドライブ１０２が暗号化ディスクキーＥｍ（Ｋｄ）２１２をメディア２０１から読み出し、ＡＥＳ＿Ｄ２２３において、メディアキーＫｍによってディスクキーＫｄが得られる。ＡＥＳ(Advanced Encryption Standard)は、米国政府がＤＥＳに代わる新しい暗号化標準として採用した暗号化方法である。

さらに、ドライブ１０２は、メディア２０１からディスクＩＤ２１３を読み出し、ＡＥＳ＿Ｇ２２４において、ディスクＩＤとディスクキーＫｄを演算し、エンベディッドキーＫｅを得る。

ドライブ１０２とホスト１０３の認証が完了し、セッションキーＫｓが得られているならば、ホスト１０３がドライブ１０２に対してエンベディッドキーＫｅの転送を要求する。

ドライブ１０２がインターフェース１０４を経由してホスト１０３に対してＫｅを転送する際に、ＡＥＳエンクリプタ２２６にてセッションキーＫｓによりＫｅを暗号化する。ホスト１０３は、ＡＥＳデク

リプタ２２８によって復号を行い、Ｋｅを得る。ＡＥＳエンクリプタ２２６およびＡＥＳデクリプタ２２８は、例えばＣＢＣ(Cipher Block Chaining)モードの処理を行う。

ホスト１０３は、コンテンツを暗号化ユニット単位で処理する。ホスト１０３は、暗号化ユニットのユニットキー生成用値Ｖｕ２１４をドライブ１０２から読み出す。ＡＥＳ＿Ｇ２２９において、エンベディッドキーＫｅとユニットキー生成用値Ｖｕ２１４とＣＣＩ２３２とからユニットキーＫｕが計算される。ユニットキーＫｕの生成にＣＣＩ２３２を用いることで、コンテンツの著作権がより強固に保護される。

ホスト１０３は、暗号化モジュール２３０において、コンテンツをユニットキーＫｕで暗号化する。暗号化コンテンツ１１３がドライブ１０２へ伝送され、記録可能なメディア２０１に記録される。

次に、第１３図を参照してこの発明の他の実施形態のプレイヤについて説明する。プレイヤは、ＲＯＭタイプのメディア２１０例えばＲＯＭディスクを再生する例である。

ＲＯＭタイプのメディア２１０には、予めコンテンツが記録されている。ホスト１０３では、暗号化の処理が不要となり、復号モジュール２３１が使用される。メディア２１０から読み出された暗号化コンテンツが復号モジュール２３１にて復号され、ＡＶコンテンツが得られる。

ＲＯＭタイプのメディア２１０の場合では、メディアキーＫｍおよびディスクキーＫｄがコンテンツ毎に固有の鍵情報である。各コンテンツは、１または複数の暗号化ユニットから構成される。

メディア２１０上にエンベディッドキー生成値Ｖｅ２１５が記録されている。エンベディッドキー生成値Ｖｅ２１５は、ディスク製造工

場でスタンパー（フォトレジストを現像したディスク原盤またはディスク原盤から最初に作成されたスタンパーを意味する）毎に、記録されたゼロでない値である。物理的ウォーターマークとして、通常のデータ記録とは、別の手段でディスク上に記録される。

エンベディッドキーＫｅは、一実施形態におけるメディアユニークキーに相当する。エンベディッドキーＫｅを生成するためのエンベディッドキー生成値Ｖｅ２１５は、一種のメディアＩＤである。

第１３図のレコーダは、第１２図に示すプレイヤと同様の処理を行う。最初にＡＫＥ２２５および２２７による認証がなされ、セッションキーＫｓが生成される。読み出されたＥＫＢ２１１とデバイスキー２２１がドライブ１０２のプロセスＥＫＢ２２２で演算され、メディアキーＫｍが算出とリボーク処理がなされる。そして、ＡＥＳ＿Ｄ２２３において、メディアキーＫｍによってディスクキーＫｄが復号される。さらに、ＡＥＳ＿Ｇ２２４において、エンベディッドキーＫｅが得られる。

ＡＥＳエンクリプタ２２６にてセッションキーＫｓによりＫｅが暗号化される。ホスト１０３は、ＡＥＳデクリプタ２２８によって復号を行い、Ｋｅを得る。

ホスト１０３は、読み出したい暗号化ユニットのユニットキー生成用値Ｖｕ２１４およびコピー制御情報ＣＣＩをドライブ１０２から読み出し、ＡＥＳ＿Ｇ２２９において、ユニットキーＫｕが計算される。

ホスト１０３が要求した暗号化ユニットのセクタデータがホスト１０３の復号モジュール２３１において、属する暗号化ユニットのユニットキーＫｕで復号される。

この発明では、著作権保護技術に関する秘密情報である電子機器ま

たはアプリケーションソフトウェア固有の情報例えばデバイスキーが記録再生装置内に実装されているので、ＤＶＤ処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報を持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

電子機器またはアプリケーションソフトウェア固有の情報としてのデバイスキーを記録再生装置とデータ処理装置が分けて持つことによって、記録再生装置およびアプリケーションソフトウェアの両方について、リボーク処理を行うことが可能となる。

この発明では、著作権保護技術に関するアルゴリズムの一部例えばメディアユニークキーの演算が記録再生装置内に実装されている。したがって、データ処理装置のアプリケーションソフトウェアは、著作権保護技術に関するアルゴリズムの一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばタイトルキーは、タイトル毎のキーであるが、この発明では、乱数情報であれば、タイトル毎に異なることは、必要ではない。

また、上述した説明においては、著作権保護技術としてＣＰＲＭおよびＣＰＲＭを拡張した例を挙げたが、ＣＰＲＭ以外の著作権保護技術に対してもこの発明を適用することができる。例えば、特開２００１－３５２３２２号公報において提案されるツリー構造の鍵配布構成

に基づく著作権保護技術に対して適用可能である。また、ＰＣベースのシステムに対してこの発明が適用されるが、このことは、ＰＣとドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

この発明では、再生装置側でコンテンツキーを生成し、コンテンツキーを情報処理装置へ送信し、情報処理装置側でコンテンツキーによってコンテンツを暗号化している。このように著作権保護のための鍵情報の生成を再生装置で行うので、ハードウェア構成でコンテンツキーを生成することが可能となり、耐タンパー性を高めることができる。また、再生装置において、乱数を生成し、乱数を中間鍵とするので、再生装置において、真正乱数またはそれに近い乱数をハードウェア例えばＬＳＩによって発生することができ、生成した乱数を固定値への置き換えを困難とすることができる。このように、この発明では、情報処理装置にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報の全てを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持たせることが容易に実施でき、また、ディスクからのデータとしてそのまま読み出された暗号化コンテンツが「ＤｅＣＳＳ」のような解読ソフトウェアにより復号され、平文のままのクリア・コンテンツとしてコピー制限の働かない状態で複製が繰り返されるような事態を防ぐことができることから、著作権保護技術の安全性を確保することができる。

また、電子機器固有の情報としてのデバイスキーを記録再生装置が

持つことによって、記録再生装置自身をリボークすることが可能となる。さらに、この発明では、情報処理装置におけるコンテンツキーを計算するのに必要とされる乱数情報が記録再生装置内の例えばＬＳＩによって生成できるので、ＰＣ内でソフトウェアによって乱数を生成するのと比較して、真正または真正乱数に近い乱数を生成することができる。したがって、乱数が固定値に置き換えられる、等のおそれを少なくできる。

請 求 の 範 囲

1．記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達部を介して相互認証接続される情報処理装置とを備える信号処理システムであって、

上記再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、

上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第1の送信部と、

上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第2の送信部とを有し、

上記情報処理装置は、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化部と、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録部とを有する信号処理システム。

2．請求の範囲1において、

上記再生装置は、

乱数を生成する乱数生成部を有し、

上記中間鍵情報は、

上記乱数生成部により生成された乱数である信号処理システム。

3．記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達部を介して相互認証接続される

情報処理装置とが、上記記録媒体に情報を記録する記録方法であって、

上記再生装置は、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第1の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第2の送信ステップとを有し、

上記情報処理装置は、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録ステップとを有する記録方法。

4．請求の範囲3において、

上記再生装置は、

乱数を生成する乱数生成ステップを有し、

上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数である記録方法。

5．記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達部を介して相互認証接続される情報処理装置とが、上記記録媒体に情報を記録するプログラムであって、

上記再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成ステップと、

上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第1の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第2の送信ステップとを行わせ、

上記情報処理装置に、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録ステップとを行わせるプログラム。

6．請求の範囲5において、

上記再生装置に、

乱数を生成する乱数生成ステップを行わせ、

上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数であるプログラム。

7．記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と、上記再生装置が伝達部を介して相互認証接続される情報処理装置とが、上記記録媒体に情報を記録するプログラムを格納した記録媒体であって、

上記再生装置に、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号

化鍵生成ステップと、

上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第1の送信ステップと、

上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第2の送信ステップを行わせ、

上記情報処理装置に、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化ステップと、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化ステップと、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録ステップとを行わせるプログラムを格納した記録媒体。

8．請求の範囲7において、

上記再生装置に、

乱数を生成する乱数生成ステップを行わせ、

上記中間鍵情報は、

上記乱数生成ステップにより生成された乱数であるプログラムを格納した記録媒体。

9．記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出し、伝達部を介して情報処理装置と接続される再生装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、

上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第1の送信部と、

上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第２の送信部とを有し、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化部と、暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報とを上記記録媒体に記録する記録部とを有する上記情報処理装置と相互認証接続される再生装置。

１０．請求の範囲９において、

乱数を生成する乱数生成部を有し、

上記中間鍵情報は、

上記乱数生成部により生成された乱数である再生装置。

１１．記録媒体固有の情報をあらかじめ備えた記録媒体から情報を読み出す再生装置と伝達部を介して接続される情報処理装置であって、

中間鍵情報に基づいてコンテンツ情報暗号化鍵を生成する最終暗号化鍵生成部と、上記中間鍵情報を上記伝達部を介して上記情報処理装置へ送る第１の送信部と、上記コンテンツ情報暗号化鍵を上記伝達部を介して上記情報処理装置へ送る第２の送信部とを有する上記再生装置と伝達部を介して相互認証接続され、

上記コンテンツ情報暗号化鍵によりコンテンツ情報を暗号化するコンテンツ情報暗号化部と、

上記記録媒体固有の情報に基づいて生成される記録媒体固有の鍵情報を用いて上記中間鍵情報を暗号化する中間鍵情報暗号化部と、

暗号化された上記コンテンツ情報および暗号化された上記中間鍵情報を上記記録媒体に記録する記録部とを有する情報処理装置。

１２．請求の範囲１１において、

上記再生装置は、

乱数を生成する乱数生成部を有し、

上記中間鍵情報は、

上記乱数生成部により生成された乱数である情報処理装置。

１３．不正な電子機器を無効化するための第１の情報と、コンテンツ毎に異なる第２の情報と、暗号化単位毎に定義可能な第３の情報と、スタンパ毎に異なる識別データとが記録された記録媒体へ暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第４の情報が格納される格納部と、

上記第１の情報と上記第４の情報とから当該格納された第４の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であるかを判定するリボーク処理部と、

上記リボーク処理部で上記第４の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報であると判定された場合に、上記第１の情報、上記第４の情報、上記第２の情報および上記識別データから、個々の記録媒体毎に固有の中間鍵情報を求める演算部と、

上記中間鍵情報を伝達部を介して情報処理装置の最終暗号化鍵生成部へ送る送信部とを有する再生装置。

１４．請求の範囲１３において、

上記中間鍵情報に基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う認証部と、

上記認証が成立した場合に形成されるセッションキーによって上記

中間鍵情報を暗号化して上記データ処理装置に送出する中間鍵情報暗号化部とを有する記録再生装置。

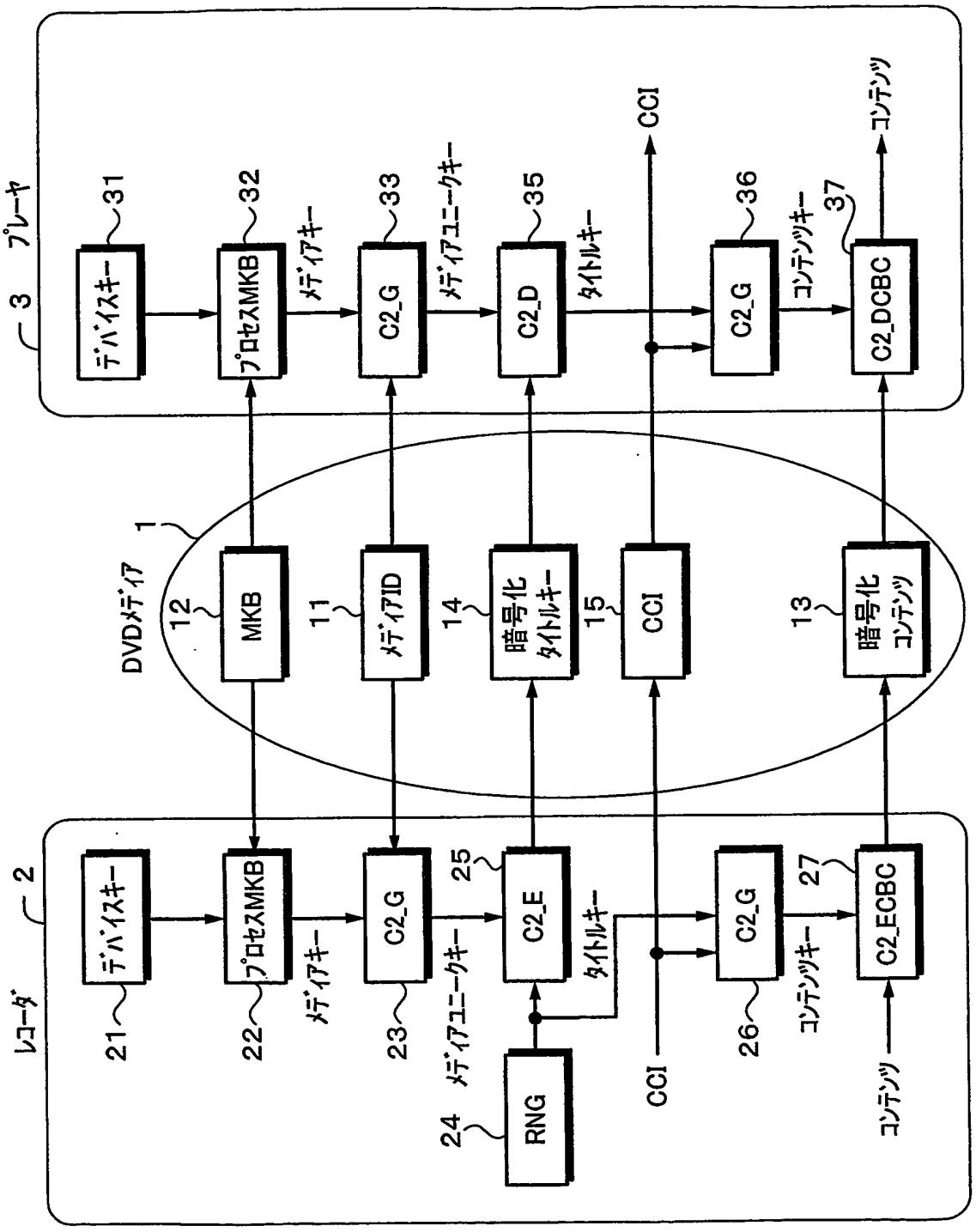
１５．正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第４の情報を有するとともに、不正な電子機器を無効化するための第１の情報と、コンテンツ毎に異なる第２の情報と、暗号化単位毎に定義可能な第３の情報と、スタンパ毎に異なる識別データとが記録された記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置との認証を行う認証部と、

上記記録再生装置から、上記認証が成立した場合に形成されるセッションキーによって暗号化された、上記第１の情報、上記第４の情報、上記第２の情報および上記識別データから生成された個々の記録媒体毎に固有の中間鍵情報を受け取り、当該中間鍵情報を復号する鍵情報復号部と、

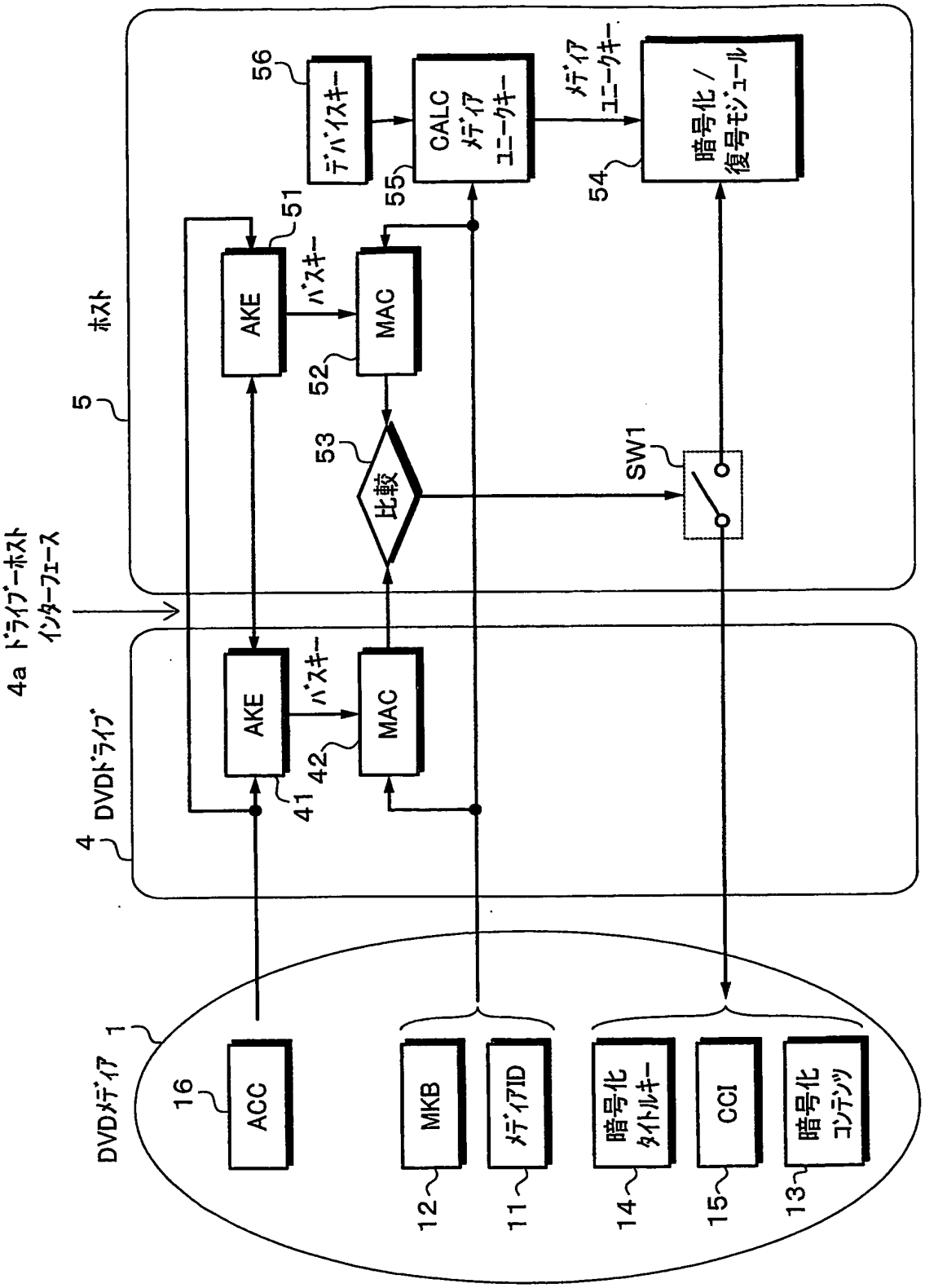
上記記録再生装置から受け取った上記第３の情報と、復号された上記中間鍵情報から最終暗号化鍵を生成する最終暗号化鍵生成部と、

上記最終暗号化鍵による暗号化と上記最終暗号化鍵による復号との少なくとも一方を行う暗号化復号部とを有するデータ処理装置。

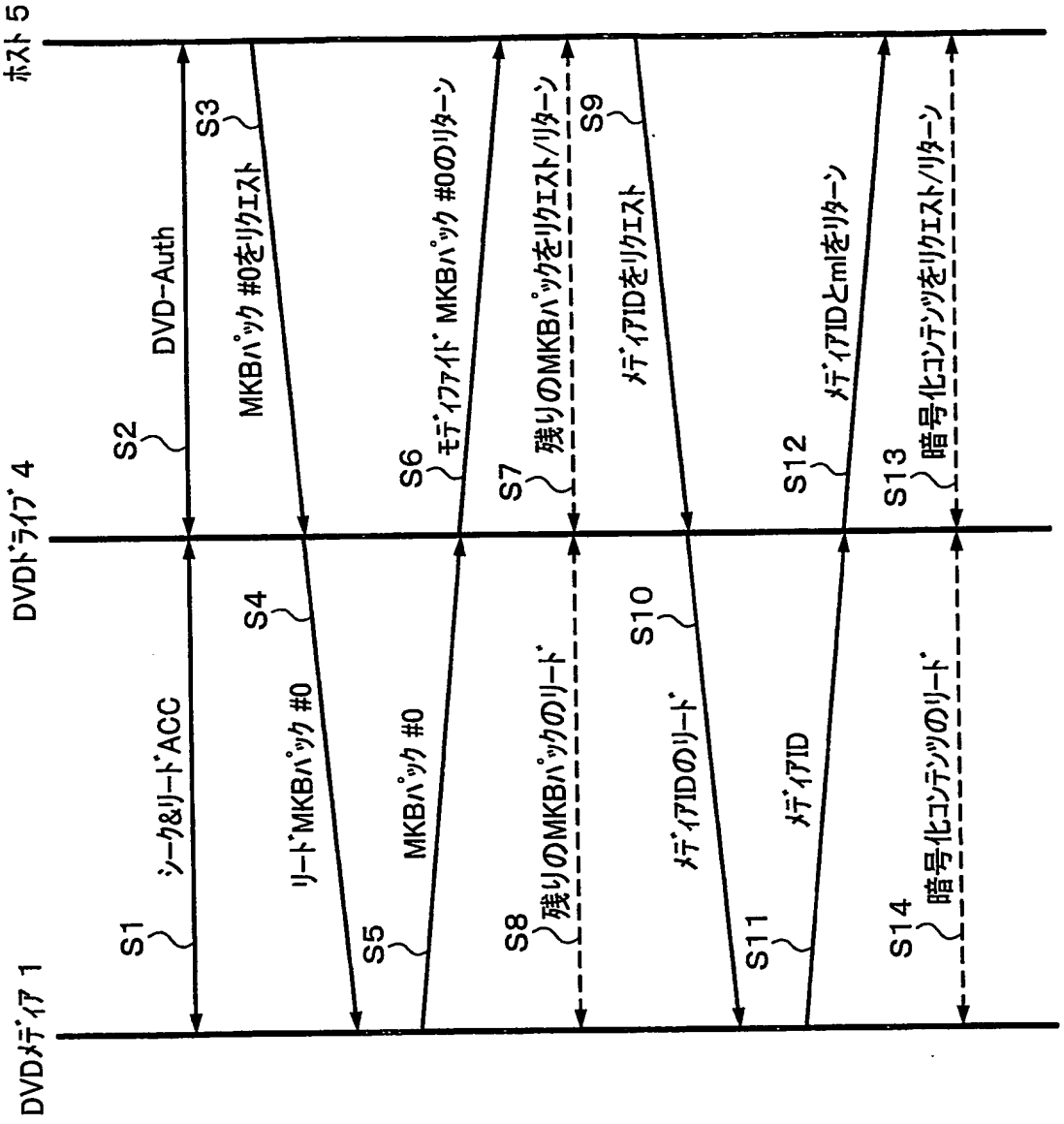
第１図


3 プレーヤ
デバイスキー 31
プロセスMKB 32
メディアキー
C2_G 33
メディアユニークキー
C2_D 35
タイトルキー
CCI
C2_G 36
コンテンツキー 37
C2_DCBC
コンテンツ
DVDメディア 1
MKB 12
メディアID 11
暗号化タイトルキー 14
CCI 15
暗号化コンテンツ 13
2 レコーダ
デバイスキー 21
プロセスMKB 22
メディアキー
C2_G 23
メディアユニークキー
C2_E 25
タイトルキー
RNG 24
CCI
C2_G 26
コンテンツキー
C2_ECBC 27
コンテンツ

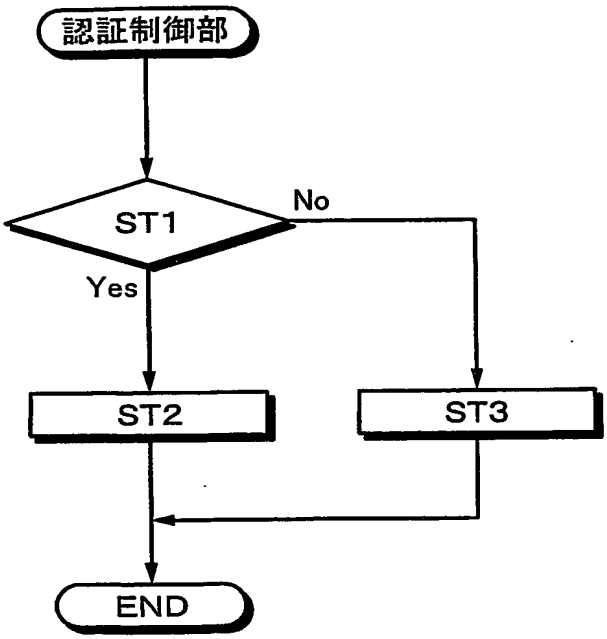
第2図


DVDメディア
1
16
ACC
MKB
12
メディアID
11
暗号化タイトルキー
14
CCI
15
暗号化コンテンツ
13
4a ドライブ-ホスト インターフェース
4 DVDドライブ
AKE
41
バスキー
MAC
42
5 ホスト
AKE
51
バスキー
MAC
52
53
比較
SW1
デバイスキー
56
CALC メディア ユニークキー
55
メディア ユニークキー
暗号化/復号モジュール
54

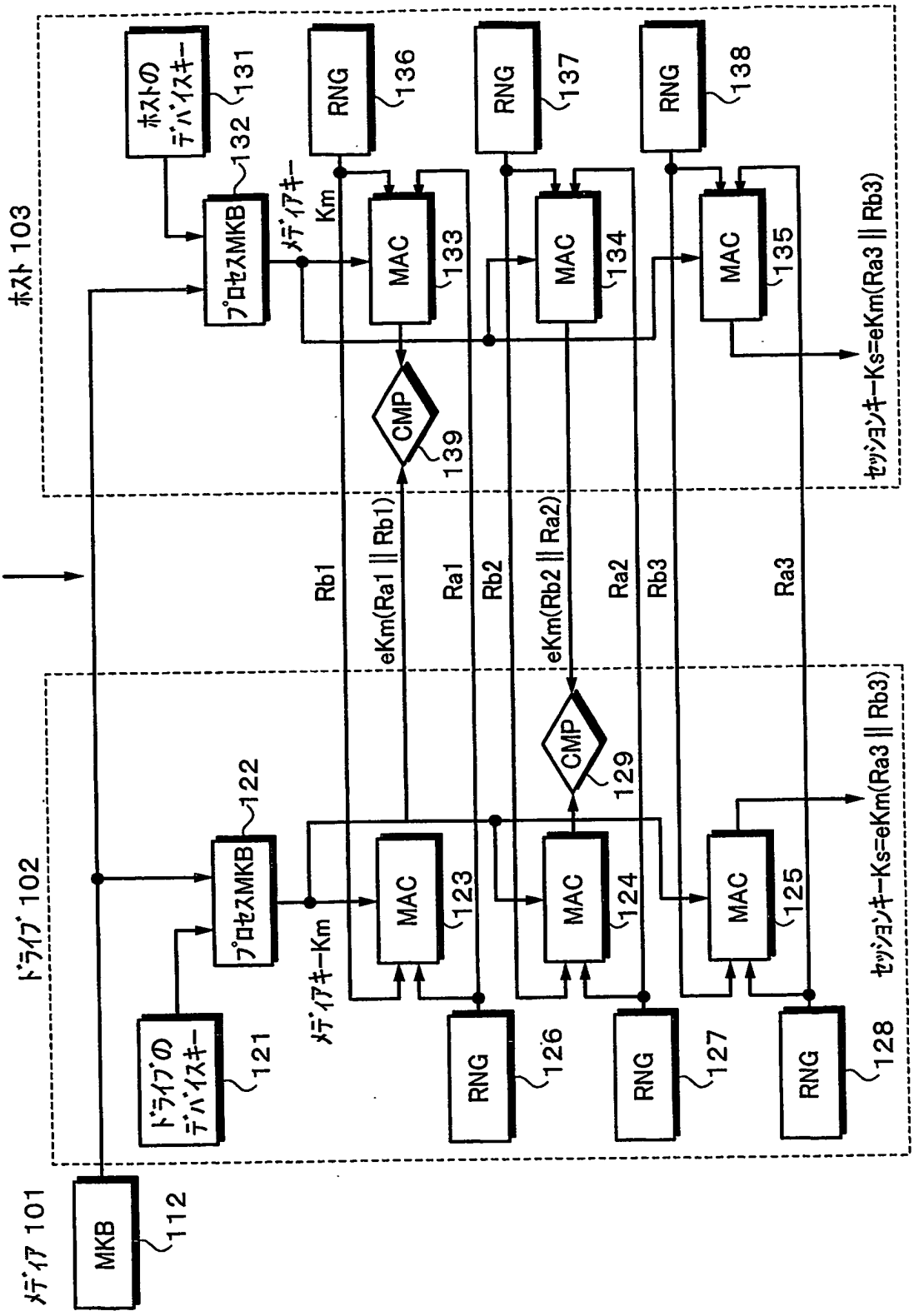
第3図


ホスト 5
DVDドライブ 4
DVDメディア 1
S1
シーク&リードACC
S2
DVD-Auth
S3
MKBパック #0をリクエスト
S4
リードMKBパック #0
S5
MKBパック #0
S6
モディファイド MKBパック #0のリターン
S7
残りのMKBパックをリクエスト/リターン
S8
残りのMKBパックのリード
S9
メディアIDをリクエスト
S10
メディアIDのリード
S11
メディアID
S12
メディアIDとmlをリターン
S13
暗号化コンテンツをリクエスト/リターン
S14
暗号化コンテンツのリード

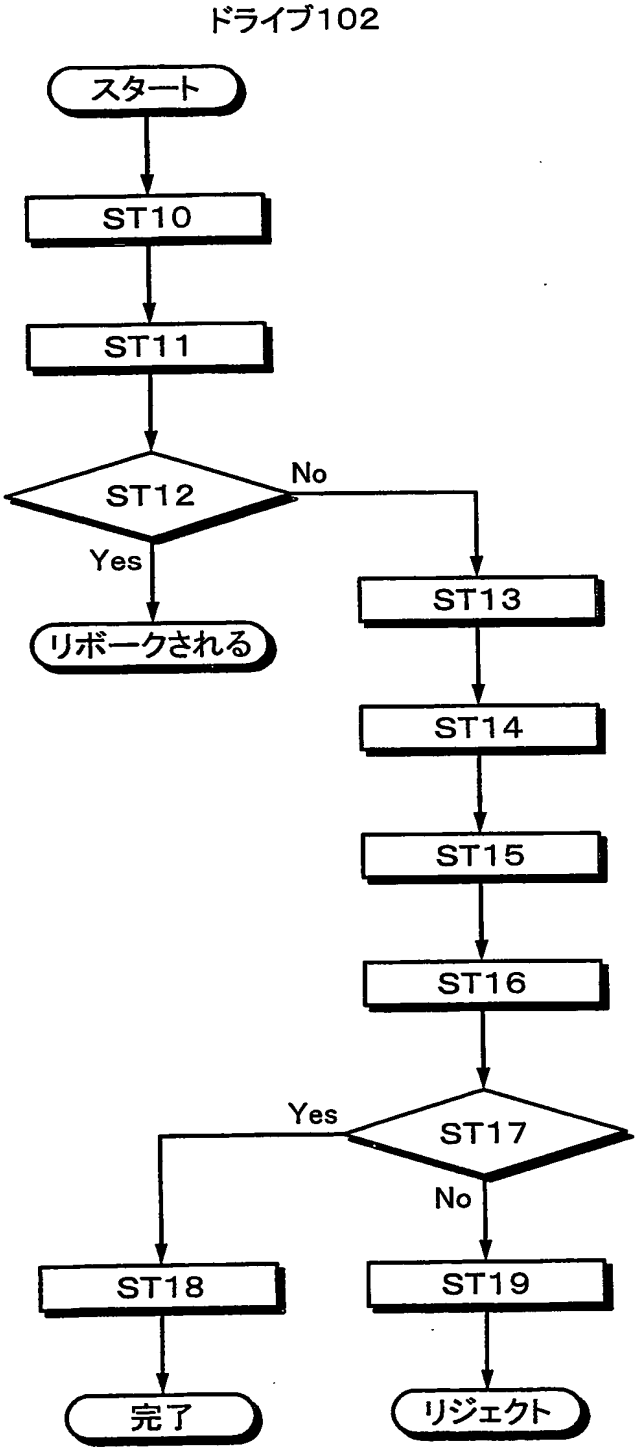
第４図



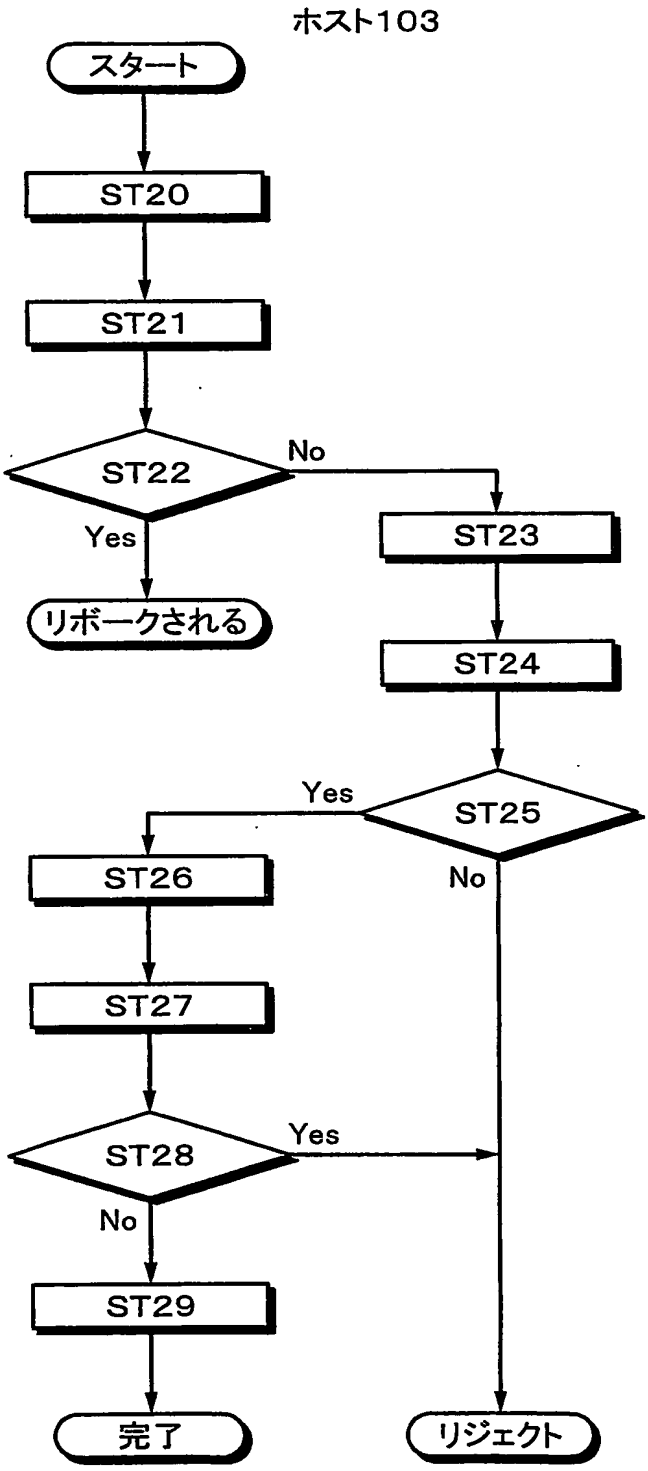
第5図


メディア 101
MKB
112
ドライブ 102
ドライブの デバイスキー
121
プロセスMKB
122
メディアキー-Km
MAC
123
MAC
124
MAC
125
RNG
126
RNG
127
RNG
128
CMP
129
eKm(Rb2 || Ra2)
Rb2
Ra2
Rb3
Ra3
ドライブ - ホストI/F 104
ホスト 103
ホストの デバイスキー
131
プロセスMKB
132
メディアキー Km
MAC
133
MAC
134
MAC
135
RNG
136
RNG
137
RNG
138
CMP
139
eKm(Ra1 || Rb1)
Rb1
Ra1
セッションキー-Ks=eKm(Ra3 || Rb3)
セッションキー-Ks=eKm(Ra3 || Rb3)

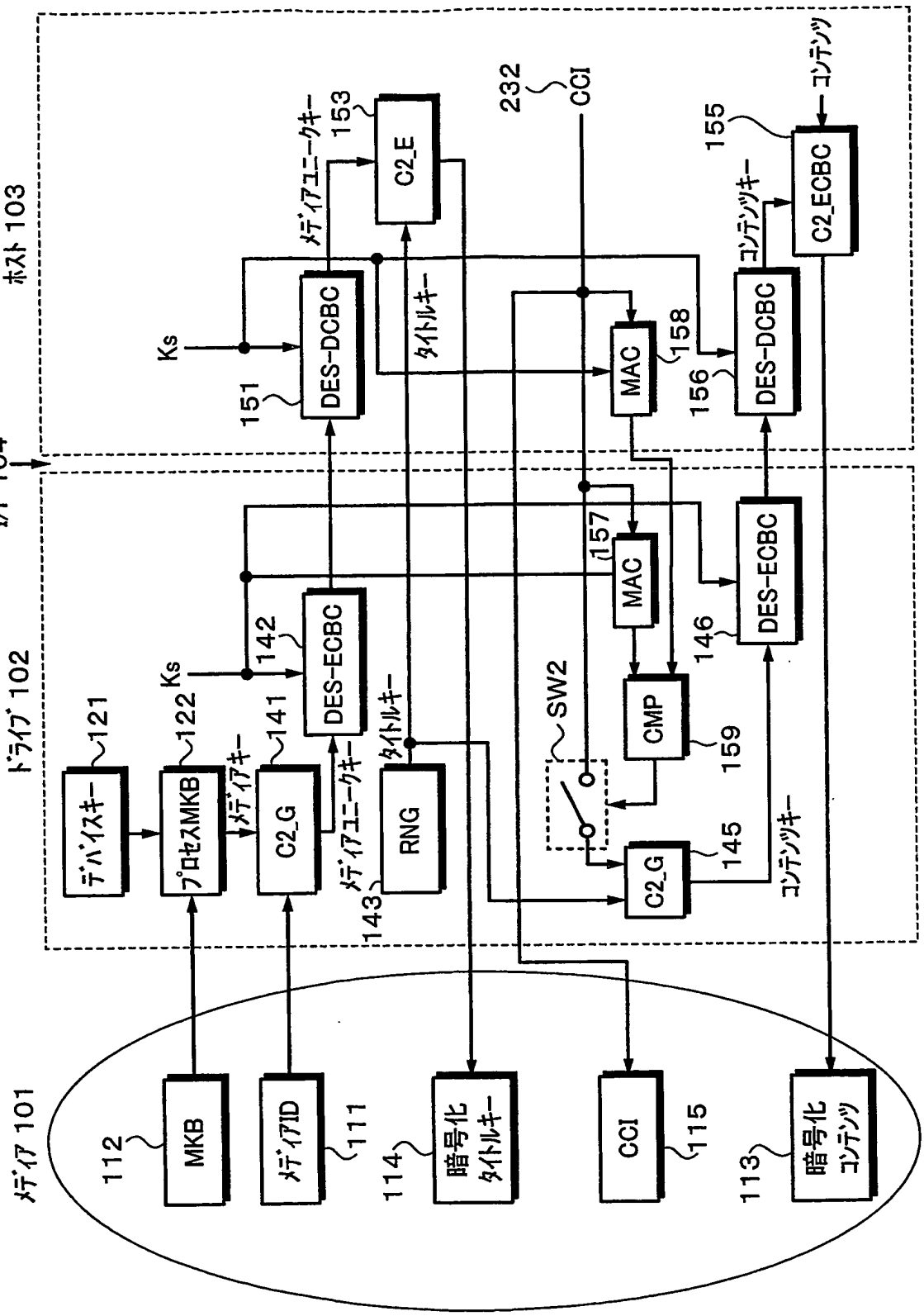
第６図


ドライブ102
スタート
ST10
ST11
ST12
No
Yes
リボークされる
ST13
ST14
ST15
ST16
Yes
ST17
No
ST18
ST19
完了
リジェクト

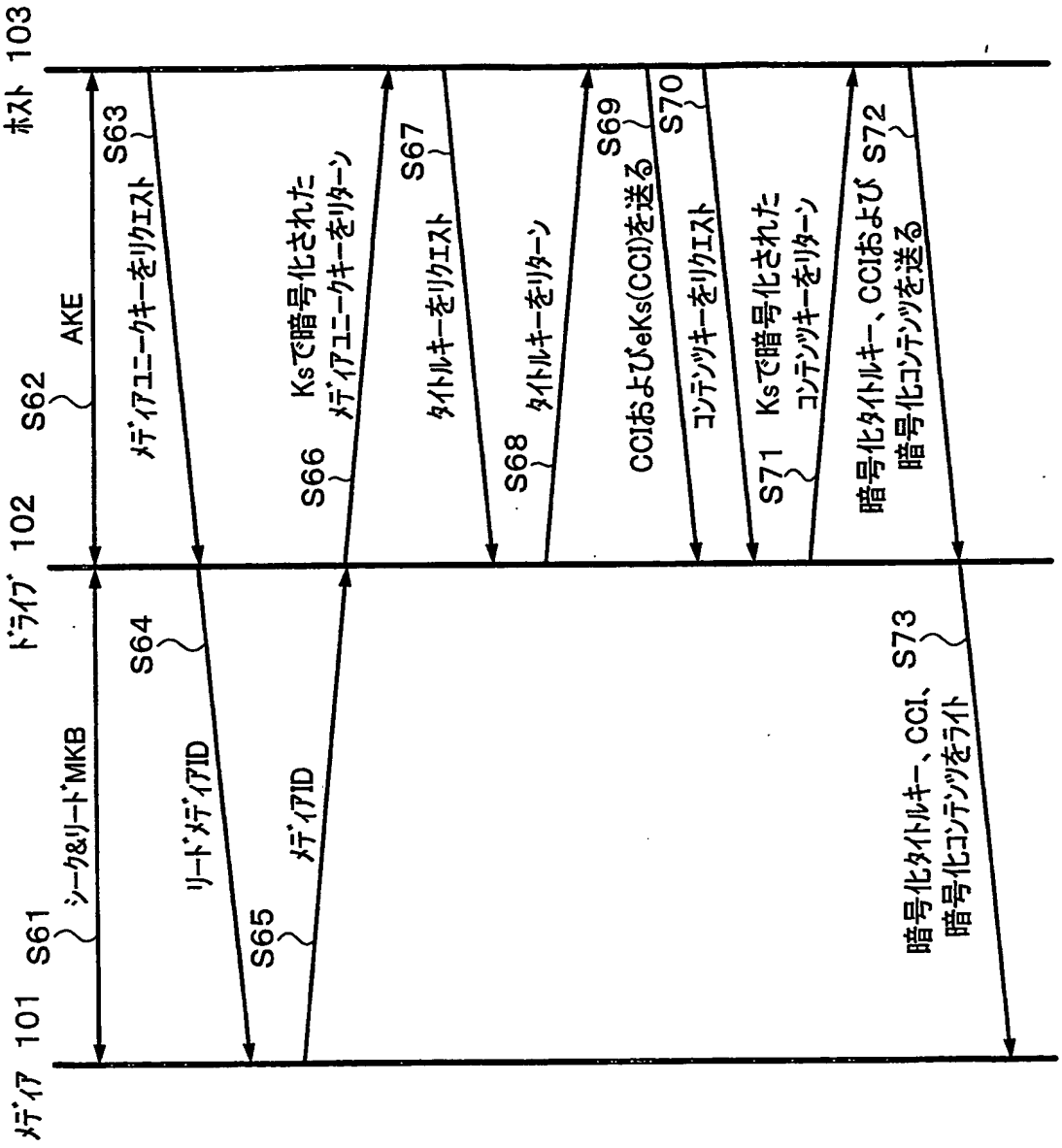
第７図


ホスト103
スタート
ST20
ST21
ST22
No
Yes
リボークされる
ST23
ST24
ST25
Yes
No
ST26
ST27
ST28
Yes
No
ST29
完了
リジェクト

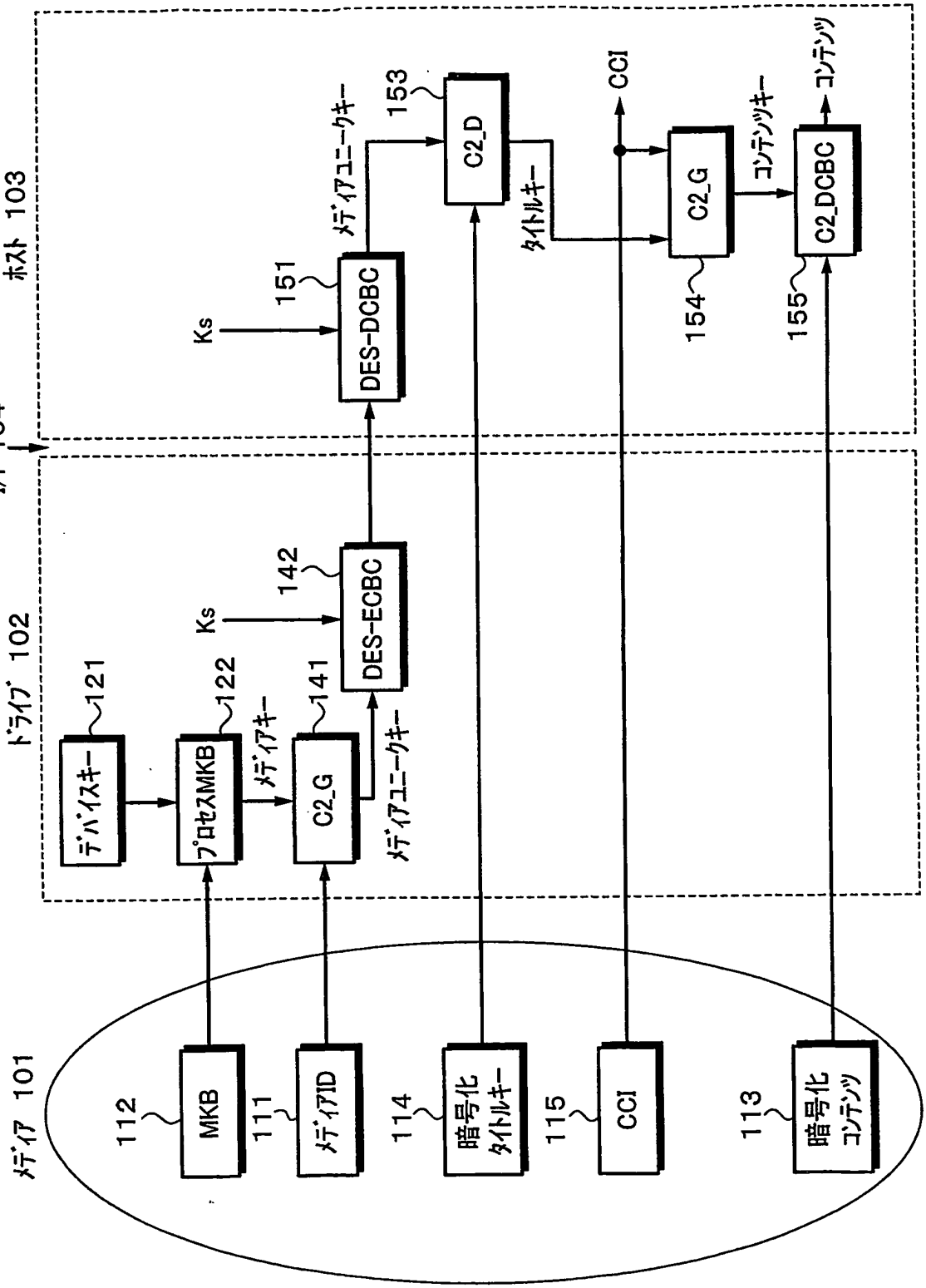
第８図


メディア 101
MKB
112
メディアID
111
暗号化タイトルキー
114
CCI
115
暗号化コンテンツ
113
I/F 104
ドライブ 102
デバイスキー
121
プロセスMKB
122
メディアキー
C2_G
141
DES-ECBC
142
メディアユニークキー
RNG
143
タイトルキー
Ks
SW2
C2_G
145
CMP
159
MAC
157
DES-ECBC
146
コンテンツキー
ホスト 103
DES-DCBC
151
メディアユニークキー
C2_E
153
タイトルキー
Ks
232
CCI
MAC
158
DES-DCBC
156
コンテンツキー
C2_ECBC
155
コンテンツ

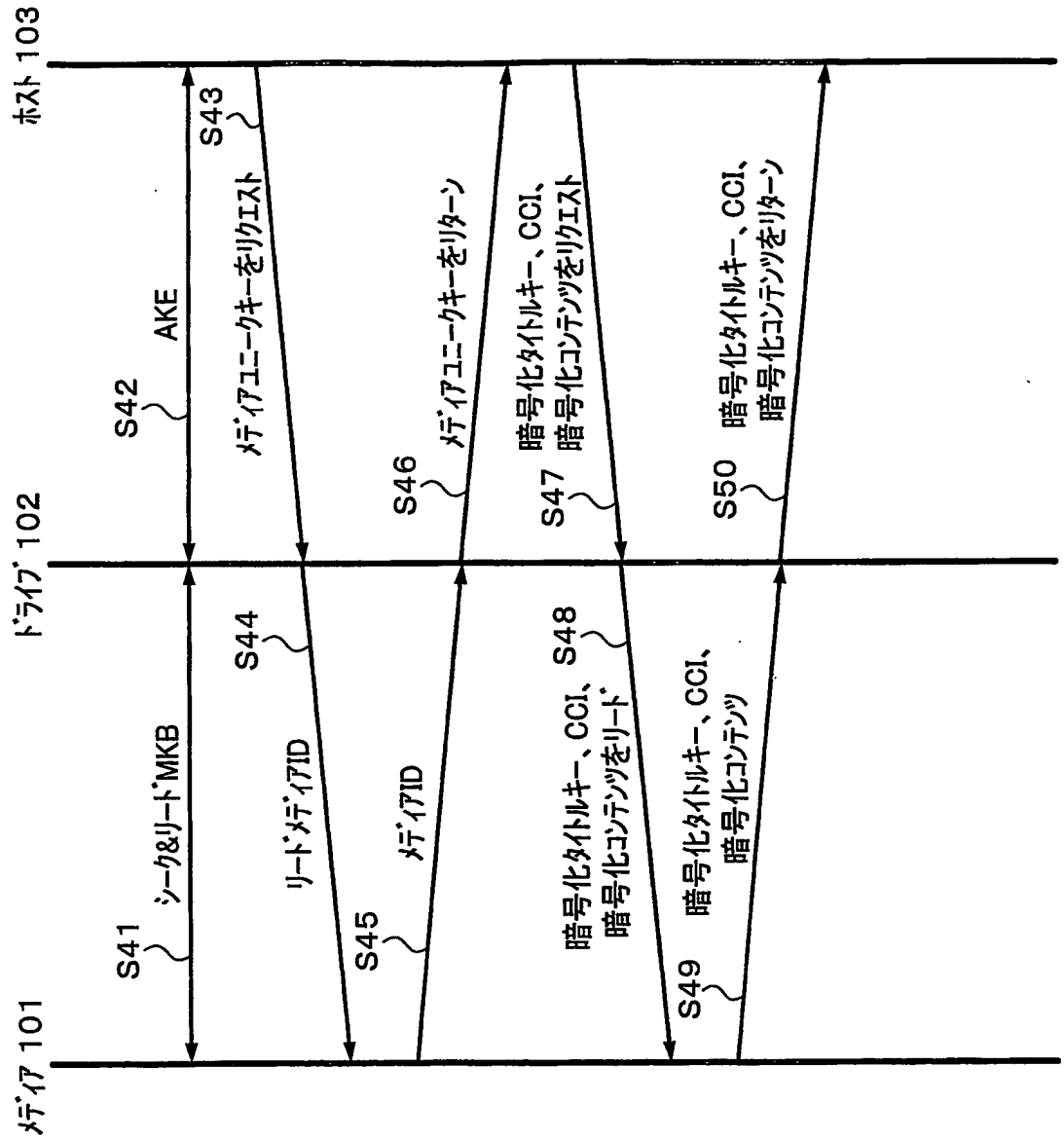
第9図


メディア 101
ドライブ 102
ホスト 103
S61
シーク&リードMKB
S62
AKE
S63
メディアユニークキーをリクエスト
S64
リードメディアID
S65
メディアID
S66
Ksで暗号化されたメディアユニークキーをリターン
S67
タイトルキーをリクエスト
S68
タイトルキーをリターン
S69
CCIおよびeKs(CCI)を送る
S70
コンテンツキーをリクエスト
S71
Ksで暗号化されたコンテンツキーをリターン
S72
暗号化タイトルキー、CCIおよび暗号化コンテンツを送る
S73
暗号化タイトルキー、CCI、暗号化コンテンツをライト

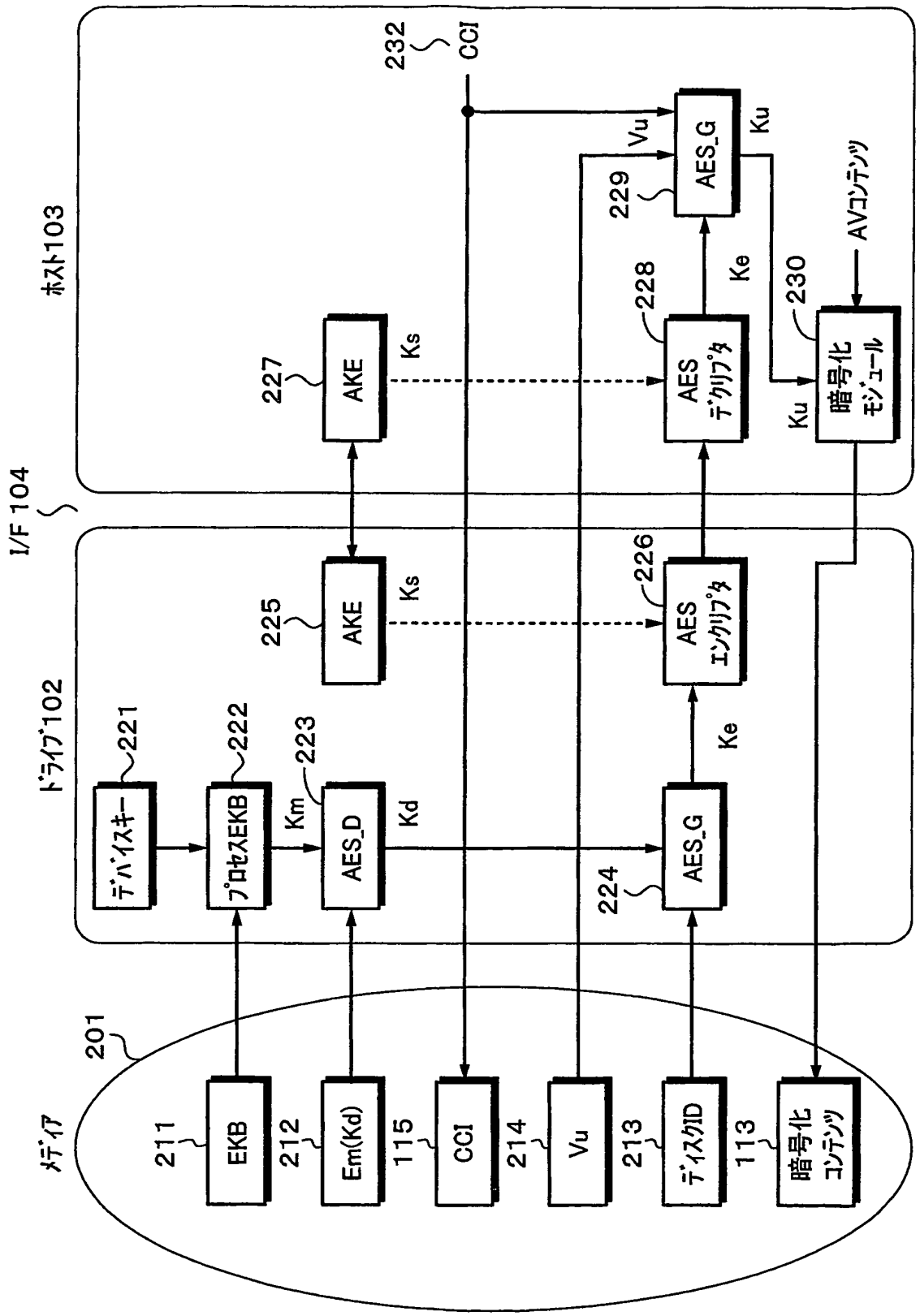
第１０図


メディア 101
MKB
112
メディアID
111
暗号化タイトルキー
114
CCI
115
暗号化コンテンツ
113
I/F 104
ドライブ 102
デバイスキー
121
プロセスMKB
122
メディアキー
C2_G
141
メディアユニークキー
DES-ECBC
142
Ks
ホスト 103
Ks
151
DES-DCBC
メディアユニークキー
153
C2_D
タイトルキー
CCI
C2_G
154
コンテンツキー
C2_DCBC
155
コンテンツ

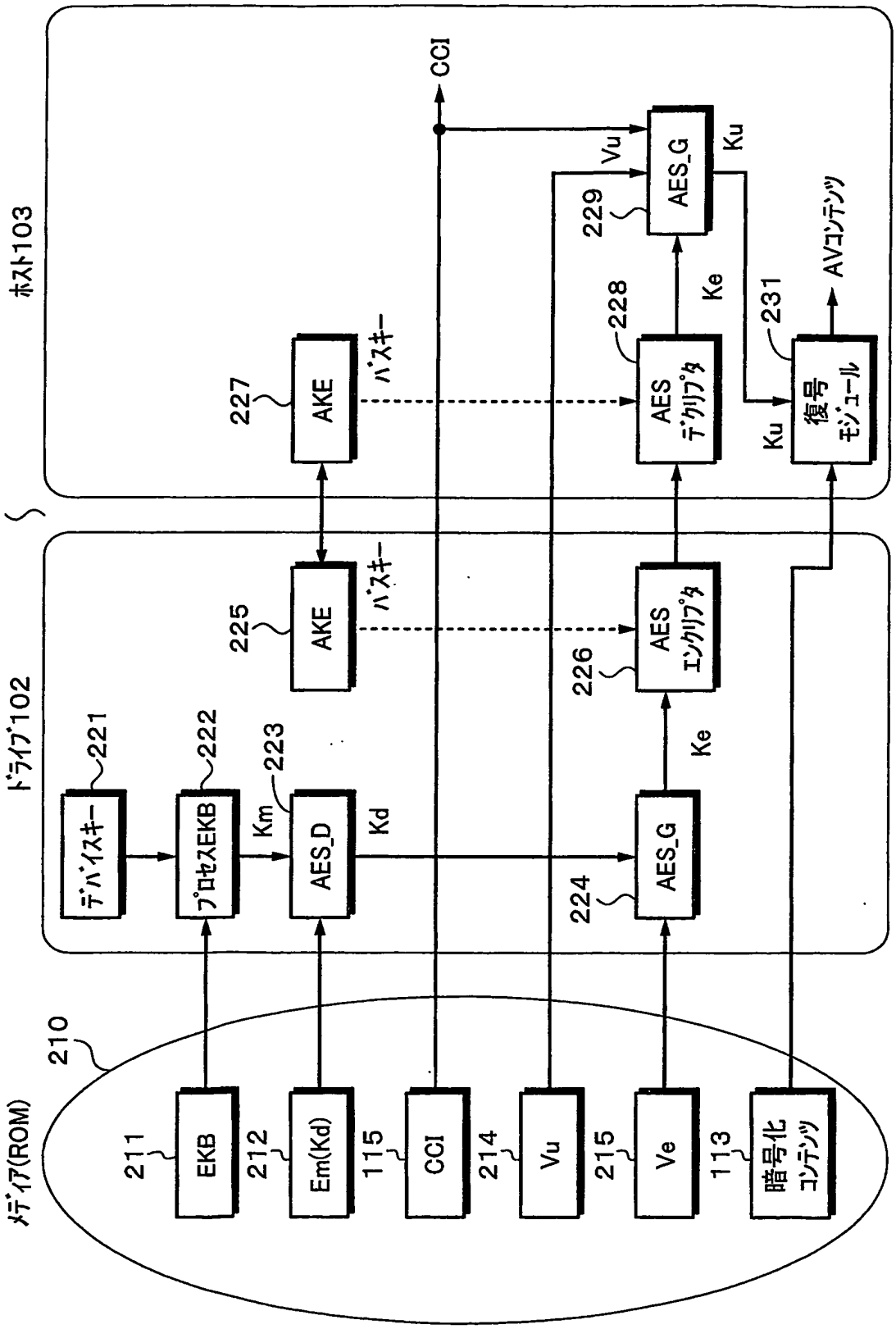
第１１図


ホスト 103
ドライブ 102
メディア 101
S41
シーク&リード MKB
S42
AKE
S43
メディアユニークキーをリクエスト
S44
リード メディアID
S45
メディアID
S46
メディアユニークキーをリターン
S47
暗号化タイトルキー、CCI、
暗号化コンテンツをリクエスト
S48
暗号化タイトルキー、CCI、
暗号化コンテンツをリード
S49
暗号化タイトルキー、CCI、
暗号化コンテンツ
S50
暗号化タイトルキー、CCI、
暗号化コンテンツをリターン

第１２図


メディア
201
211
EKB
212
Em(Kd)
115
CCI
214
Vu
213
ディスクID
113
暗号化コンテンツ
ドライブ102
221
デバイスキー
222
プロセスEKB
223
Km
AES_D
Kd
225
AKE
Ks
224
AES_G
Ke
226
AES エンクリプタ
I/F 104
ホスト103
227
AKE
Ks
228
AES デクリプタ
Ke
229
AES_G
Ku
230
暗号化モジュール
Ku
AVコンテンツ
232
CCI
Vu

第１３図


メディア(ROM)
210
211
EKB
212
Em(Kd)
115
CCI
214
Vu
215
Ve
113
暗号化コンテンツ
ドライブ102
デバイスキー
221
プロセスEKB
222
Km
223
AES_D
Kd
225
AKE
バスキー
224
AES_G
Ke
226
AES デクリプタ
I/F 104
ホスト103
227
AKE
バスキー
CCI
Vu
229
AES_G
Ku
228
AES デクリプタ
Ke
231
復号モジュール
Ku
AVコンテンツ

符号の説明

1　ＤＶＤメディア
2　レコーダ
3　プレーヤ
4　ＤＶＤドライブ
4ａ　インターフェース
5　ホスト
１１１　メディアＩＤ
１１２　メディアキーブロック（ＭＫＢ）
１１３　暗号化コンテンツ
１０１　メディア
１０２　ドライブ
１０３　ホスト
１０４　インターフェース
１２１　ドライブのデバイスキー
１２２　プロセスＭＫＢ
１２３、１２４、１２５　ドライブのＭＡＣ演算ブロック
１２６、１２７、１２８　ドライブの乱数発生器
１２９　比較
１３１　ホストのデバイスキー
１３２　プロセスＭＫＢ
１３３、１３４、１３５　ホストのＭＡＣ演算ブロック
１３６、１３７、１３８　ホストの乱数発生器
１３９　比較
１４１、１５４　Ｃ２＿Ｇ

142、146　DESエンクリプタ

143　乱数発生器

151、152、156　DESデクリプタ

153　C2_E

155　C2_EBC

157、158　MAC演算ブロック

159　比較

ST1　MAC計算値が一致？

ST2　スイッチをON

ST3　スイッチをOFF

ST10　REPORT KEY（MKB）

ST11　メディアキーKmを計算

ST12　リボーク？

ST13　RECEIVE（Rb1，Rb2）

ST14　RETURN（eKm(Ra1‖Rb1)，Ra1）

ST15　RETURN（Ra2，Ra3）

ST16　RECEIVE
（eKm(Rb2‖Ra2)，Rb3）

ST17　同一のMAC？

ST18　セッションキーの確定
（eKm(Ra3‖Rb3)）

ST19　RETURN（エラー）

ST20　REPORT KEY（MKB）

ST21　メディアキーKmを計算

ST22　リボーク？

ST23　SEND KEY（Rb1，Rb2）

ＳＴ２４　ＲＥＰＯＲＴ　ＫＥＹ
（eＫｍ(Ｒａ１‖Ｒｂ１)，Ｒａ１）

ＳＴ２５　同一のＭＡＣ？

ＳＴ２６　ＲＥＰＯＲＴ　ＫＥＹ（Ｒａ２，Ｒａ３）

ＳＴ２７　ＳＥＮＤ　ＫＥＹ
（eＫｍ(Ｒｂ２‖Ｒａ２)，Ｒｂ３）

ＳＴ２８　エラー？

ＳＴ２９　セッションキーの確定
（eＫｍ(Ｒａ３‖Ｒｂ３)）

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/16937

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/10, G11B20/10, G11B20/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/10, G11B20/10, G11B20/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, DVD, media, cipher, encryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 9-190667 A (Toshiba Corp.), 22 July, 1997 (22.07.97), All pages & WO 97/25711 A1 & AU 9711099 A & EP 814474 A1 & TW 316301 A & KR 97706539 A & CA 2199241 C & JP 2001-292136 A & CN 1176014 A & US 6347846 B1 & US 2002/0061105 A1	1-15
A	JP 11-66706 A (Toshiba Corp.), 09 March, 1999 (09.03.99), All pages (Family: none)	1-15
A	JP 2000-100069 A (Toshiba Corp.), 07 April, 2000 (07.04.00), All pages (Family: none)	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
16 April, 2004 (16.04.04)

Date of mailing of the international search report
27 April, 2004 (27.04.04)

Name and mailing address of the ISA/
Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

国際調査報告

国際出願番号 PCT/JP03/16937

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9/10, G11B20/10, G11B20/12

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9/10, G11B20/10, G11B20/12

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI
DVD, media ,cipher, encryption

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 9-190667 A（株式会社東芝）1997.07.22, 全頁を参照 & WO 97/25711 A1 & AU 9711099 A & EP 814474 A1 & TW 316301 A & KR 97706539 A & CA 2199241 C & JP 2001-292136 A & CN 1176014 A & US 6347846 B1 & US 2002/0061105 A1	1-15
A	JP 11-66706 A（株式会社東芝）1999.03.09, 全頁を参照（ファミリなし）	1-15
A	JP 2000-100069 A（株式会社東芝）2000.04.07, 全頁を参照（ファミリなし）	1-15

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 16.04.2004	国際調査報告の発送日 27.4.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA/JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里 裕正 5M 9364 電話番号 03－3581－1101 内線 3597

様式PCT/ISA/210（第2ページ）（1998年7月）